Tsunami MP.11 Installation and Management

Model 5054 (MP.11a)

Version 4.0.0

proxim wireless

IMPORTANT!
Before installing and using this product, see the
Safety and Regulatory Compliance Guide located on the product CD.

Copyright

©2007 Proxim Wireless Corporation, San Jose, CA. All rights reserved. Covered by one or more of the following U.S. patents: 5,231,634; 5,875,179; 6,006,090; 5,809,060; 6,075,812; 5,077,753. This manual and the software described herein are copyrighted with all rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form by any means without the written permission of Proxim Wireless Corporation.

Trademarks

Tsunami, Proxim, and the Proxim logo are trademarks of Proxim Wireless Corporation. All other trademarks mentioned herein are the property of their respective owners.

Tsunami MP.11 5054 (MP.11a) Installation and Management Guide
P/N 73871 June 2007

Contents

1 Introduction . . . 9
About This Book . . . 9
Reference Manual . . . 10
Wireless Network Topologies . . . 11
Point-to-Point Link . . . 11
Point-to-Multipoint Network . . . 12
Management and Monitoring Capabilities . . . 12
Web Interface . . . 12
Command Line Interface . . . 12
SNMP Management . . . 12

2 Installation and Initialization . . . 14
Hardware Overview . . . 15
Power-over-Ethernet . . . 15
Product Package . . . 16
Installation Procedure . . . 18
Step 1: Choose a Location . . . 20
Step 2: Unpack Shipping Box . . . 20
Step 3: Attach Base (for Desktop or Ceiling Mounting only) . . . 21
Step 4: Remove Covers . . . 22
Step 5: Connect the Cables . . . 23
Step 6: Mount the Unit . . . 24
Step 7: Power on the Unit . . . 28
Step 8: View LEDs . . . 28
Step 9: Align the Antenna . . . 29
Step 10: Attach Kensington Security Lock (Optional) . . . 30
Step 11: Install Documentation and Software . . . 31
Initialization . . . 32
ScanTool . . . 32
Setting the IP Address with ScanTool . . . 32
Logging in to the Web Interface . . . 34

3 System Overview . . . 35
Changing Basic Configuration Information . . . 35
Country and Related Settings . . . 35
Dynamic Frequency Selection (DFS) . . . 36
Transmit Power Control . . . 37
SU Registration . . . 38
Dynamic Data Rate Selection (DDRS) . . . 39
Virtual Local Area Networks (VLANs) . . . 40

Quality of Service (QoS) . . . 41
Concepts and Definitions . . . 41

4 Basic Management . . . 45

Navigation . . . 45
Rebooting and Resetting . . . 46
Rebooting . . . 46
Resetting Hardware . . . 46
Soft Reset to Factory Default . . . 47
General Configuration Settings . . . 48
Monitoring Settings . . . 49
Security Settings . . . 50
Encryption . . . 50
Passwords . . . 50
Default Settings . . . 51
Upgrading the Unit . . . 53

5 System Status . . . 54

Status . . . 54
System Status . . . 54
Systems Traps . . . 54
Event Log . . . 55

6 Configuration . . . 56

System Parameters . . . 56
Bridge and Routing Modes . . . 58
Network Parameters . . . 61
IP Configuration . . . 61
Roaming . . . 62
DHCP Server . . . 65
Spanning Tree (Bridge Mode Only) . . . 67
IP Routes (Routing Mode Only) . . . 68
DHCP Relay Agent (Routing Mode Only) . . . 69
Interface Parameters . . . 71
Wireless . . . 71
Ethernet . . . 82
SNMP Parameters . . . 83
Trap Host Table . . . 83
Management Parameters . . . 85
Passwords . . . 85
Services . . . 85

Security Parameters . . . 88
MAC Authentication (BSU Only) . . . 88
Encryption . . . 89
RADIUS Authentication (BSU Only) . . . 89
Filtering Parameters . . . 91
Overview . . . 91
Ethernet Protocol . . . 92
Static MAC Address Filtering . . . 93
Storm Threshold . . . 96
Broadcast Protocol Filtering . . . 96
IP Access Table Filtering . . . 97
Intra-Cell Blocking (BSU Only; Bridge Mode Only) . . . 99
Overview . . . 99
Intra-Cell Blocking Group Table . . . 99
MAC Table . . . 101
Security Gateway . . . 102
VLAN Parameters (BSU Only; Bridge Mode Only) . . . 103
Overview . . . 103
BSU VLAN Configuration . . . 108
SU VLAN Configuration . . . 109
QoS (Quality of Service) Parameters (BSU Only) . . . 112
QoS PIR Configuration . . . 112
QoS SFC Configuration . . . 113
QoS Class Configuration . . . 115
QoS SU Configuration . . . 119
QoS Configuration for a Management Station . . . 120
RIP Parameters (Routing Mode Only) . . . 125
RIP Example . . . 126
RIP Notes . . . 126
NAT (SU Only; Routing Mode Only) . . . 127
NAT Static Port Mapping Table . . . 127
Supported Session Protocols . . . 128

7 Monitoring . . . 130

Wireless . . . 131
General Performance . . . 131
WORP Interface Performance . . . 131
ICMP . . . 133
Per Station . . . 134
Site Survey . . . 134
Features . . . 135

Link Test . . . 136
Interfaces . . . 137
IP ARP Table . . . 138
IP Routes . . . 139
Learn Table . . . 140
RIP . . . 141
RADIUS (BSU Only) . . . 142
QoS (BSU Only) . . . 143

8 Commands . . . 144
Download . . . 144
Upload . . . 145
Reboot . . . 146
Reset . . . 147
Help Link . . . 148
Downgrade . . . 149

9 Procedures . . . 150
TFTP Server Setup . . . 151
Web Interface Image File Download . . . 152
Configuration Backup . . . 153
Configuration Restore . . . 154
Soft Reset to Factory Default . . . 155
Hard Reset to Factory Default . . . 156
Forced Reload . . . 157
Image File Download with the Bootloader . . . 158
Download with ScanTool . . . 158
Download with CLI . . . 158

10 Troubleshooting . . . 160
Connectivity Issues . . . 160
Unit Does Not Boot . . . 160
Serial Link Does Not Work . . . 160
HyperTerminal Connection Problems . . . 161
Ethernet Link Does Not Work . . . 161
Cannot Use the Web Interface . . . 161
Communication Issues . . . 162
Two Units Are Unable to Communicate Wirelessly . . . 162
Setup and Configuration Issues . . . 163

Lost Password . . . 163
The Unit Responds Slowly . . . 163
Web Interface Does Not Work . . . 163
Command Line Interface Does Not Work . . . 163
TFTP Server Does Not Work . . . 163
Online Help Is Not Available . . . 164
Changes Do Not Take Effect . . . 164
VLAN Operation Issues . . . 165
Link Problems . . . 166
General Check . . . 166
Statistics Check . . . 166
Analyzing the Spectrum . . . 167

A Country Codes and Channels . . . 168
Channels/Frequencies by Country . . . 168

B Technical Specifications . . . 171
Part Numbers . . . 172
Radio Units . . . 172
Accessories . . . 174
Regulatory Approval and Frequency Ranges . . . 175
OFDM Modulation Rates . . . 177
Wireless Protocol . . . 177
Interfaces . . . 177
Receive Sensitivity . . . 177
Maximum Throughput . . . 178
Latency . . . 178
Transmit Power Settings . . . 178
Range Information . . . 179
External Antenna . . . 179
Hardware Specifications . . . 179
Software Features . . . 179
Management . . . 180
LEDs . . . 180
Power Requirements . . . 181
Physical and Environmental Specifications . . . 181
MTBF and Warranty . . . 181

C Lightning Protection . . . 182

D Technical Services and Support . . . 183

Obtaining Technical Services and Support 183
Support Options 184
Proxim eService Web Site Support 184
Telephone Support 184
ServPak Support 184

E Statement of Warranty 185

Warranty Coverage 185
Repair or Replacement 185
Limitations of Warranty 185
Support Procedures 185
Other Information 186
Search Knowledgebase 186
Ask a Question or Open an Issue 186
Other Adapter Cards 186

1 Introduction

The Tsunami MP.11 Model 5054 (MP.11a) Base Station Unit and Subscriber Unit is a flexible wireless indoor router that lets you design solutions for point-to-point links and point-to-multipoint networks.

The 5054 (MP.11a) is part of the Tsunami MP.11 product family, which is comprised of several additional products, including:

- The 954-R, 2454-R, 4954-R, 5054-R, 5054-R-LR Base Station Units (BSUs) and Subscriber Units (SUs) for outdoor installation
- The 5012-SUR Subscriber Units for outdoor installation
- The 5054-SUI and 5012-SUI Subscriber Units for indoor installation

Some of the key features of the MP.11 product family are:

- The use of a highly optimized protocol for outdoor applications
- Routing and bridging capability
- Asymmetric bandwidth management
- Management through a Web Interface, a Command Line Interface (CLI), or Simple Network Management Protocol (SNMP)
- Software and configuration upgrade through file transfer (TFTP)
- Outdoor placement, close to the antenna, for significantly improved range and ease of installation
- Optional integrated antenna
- VLAN support

About This Book

Before installing and using the unit, Proxim recommends you review the following chapters of this manual:

- **Chapter 1 “Introduction” (this chapter):** Provides an overview of the content of this manual as well as wireless network topologies and combinations that can be built with the unit.
- **Chapter 2 “Installation and Initialization”:** Provides detailed installation instructions and explains how to access the unit for configuration and maintenance.
- **Chapter 3 “System Overview”:** Provides a high-level overview of system features.
- **Chapter 4 “Basic Management”:** Explains how to navigate the user interface, and discusses the most common settings used to manage the unit.
- **Chapter 5 “System Status”:** Depicts the Web Interface’s “Status” options, including System Status and Event Logs.
- **Chapter 6 “Configuration”:** Depicts the Web Interface’s “Configure” options in a hierarchical manner, so you can easily find details about each item.
- **Chapter 7 “Monitoring”:** Depicts the Web Interface’s “Monitor” options in a hierarchical manner, so you can easily find details about each item
- **Chapter 8 “Commands”:** Depicts the Web Interface’s “Commands” options in a hierarchical manner, so you can easily find details about each item
- **Chapter 9 “Procedures”:** Provides a set of procedures, including TFTP Server Setup, Configuration Backup, Restore, and Download, Forced Reload, and Reset to Factory Defaults.
- **Chapter 10 “Troubleshooting”:** Helps you to isolate and solve problems with your radio unit.

The appendixes contain supplementary information you may not need immediately, including Country Code Tables and Technical Support information.

NOTE: *If you are already familiar with this type of product, you can use the Quick Install Guide to install the unit.*

Reference Manual

As a companion to the *Installation and Management* manual, the *Tsunami MP.11/QB.11 Reference Manual* provides the following supplemental information:

- **Command Line Interface:** Documents the text-based configuration utility's keyboard commands and parameters.
- **Event Log Error Messages:** Documents the error messages that you may see in your Event Log.
- **Alarm Traps:** Documents the alarm traps that can be set.
- **Microsoft Windows IAS Radius Server Configuration:** Provides information to assist you in setting up the IAS Radius Server.
- **Addition of Units to a Routed Network:** Describes how to add more units to your routed network.
- **Glossary:** Describes terms used in the Tsunami MP.11 documentation and in the wireless industry.

Wireless Network Topologies

The unit can be used in various network topologies and combinations. The required equipment depends upon the wireless network topology you want to build. Make sure all required equipment is available before installing the unit.

You can connect the 5054 to an outdoor antenna with an optional antenna kit. See the *Tsunami MP.11 Antenna Installation Guide* for details.

WARNING: To connect the unit to an outdoor antenna, consult the appropriate manufacturers' documentation for additional regulatory information, safety instructions, and installation requirements.

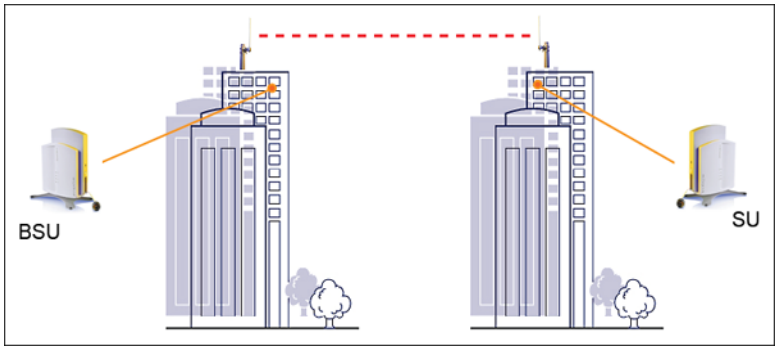
You can set up the following types of topologies:

- Point-to-Point Link
- Point-to-Multipoint Network

Each unit is set up as either a Base Station Unit (BSU) or a Subscriber Unit (SU). A link between two locations always consists of a BSU and an SU. A BSU can, depending upon its configuration, connect to one or more SUs. An SU, however, can connect to only one BSU at a time.

Point-to-Point Link

With a BSU and an SU, it is easy to set up a wireless point-to-point link as depicted in the following figure.

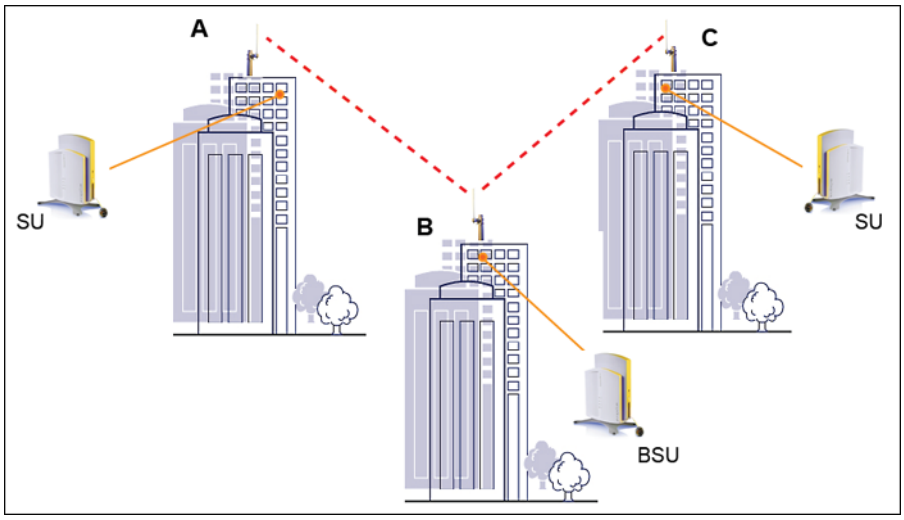


A point-to-point link lets you set up a connection between two locations as an alternative to:

- Leased lines in building-to-building connections
- Wired Ethernet backbones between wireless access points in difficult-to-wire environments

Point-to-Multipoint Network

If you want to connect more than two buildings, you can set up a single point-to-multipoint network with a single BSU and multiple SUs, as depicted in the following figure.



Up to 250 SUs can be connected to a BSU. If a BSU already has 250 SUs, a new SU cannot be connected to the BSU. In this figure, the system is designed as follows:

- The central building **B** is equipped with a BSU, connected to either an omni-directional, or a wide angle antenna.
- The two other buildings **A** and **C** are both equipped with an SU connected to a directional antenna.

Management and Monitoring Capabilities

There are several management and monitoring interfaces available to the network administrator to configure and manage the unit:

- Web Interface
- Command Line Interface
- SNMP Management

Web Interface

The Web interface (HTTP) provides easy access to configuration settings and network statistics from any computer on the network. You can access the Web interface over your network, over the Internet, or with a crossover Ethernet cable connected directly to your computer's Ethernet port. See Logging in to the Web Interface.

Command Line Interface

The Command Line Interface (CLI) is a text-based configuration utility that supports a set of keyboard commands and parameters to configure and manage the unit. You enter command statements, composed of CLI commands and their associated parameters. You can issue commands from the keyboard for real-time control or from scripts that automate configuration. See the *Tsunami MP.11/QB.11 Reference Manual* for more information about the Command Line Interface.

SNMP Management

In addition to the Web interface and the CLI, you also can manage and configure your unit using the Simple Network Management Protocol (SNMP). Note that this requires an SNMP manager program (sometimes called MIB browser) or a

Network Manager program using SNMP, such as HP OpenView or Castelrock's SNMPc. The units support several Management Information Base (MIB) files that describe the parameters that can be viewed and configured using SNMP:

- mib802.mib
- orinoco.mib
- rfc1213.mib
- rfc1493.mib
- rfc1643.mib

Proxim provides these MIB files on the CD included with your unit. You must compile one or more of these MIB files into your SNMP program's database before you can manage your unit using SNMP. See the documentation that came with your SNMP manager for instructions about how to compile MIBs.

NOTE: *When you update the software in the unit, you must also update the MIBs to the same release. Because the parameters in the MIB may have changed, you will not otherwise have full control over the features in the new release.*

The enterprise MIB (orinoco.mib) defines the read and read/write objects you can view or configure using SNMP. These objects correspond to most of the settings and statistics that are available with the other management interfaces. See the enterprise MIB for more information; the MIB can be opened with any text editor, such as Microsoft Word, Notepad, and WordPad. See SNMP Parameters.

IMPORTANT!

Using a serial connection, you can access the CLI of the unit through a terminal emulation program such as HyperTerminal. (See "HyperTerminal Connection Properties" in the *Tsunami MP.11/QB.11 Reference Manual*.)

For all other modes of connection, you will need the IP address of the unit in order to use the Web Interface, SNMP, or the CLI via telnet. See Setting the IP Address with ScanTool for more information.

IMPORTANT!

The remainder of the User Guide discusses installing the unit and managing it using the Web and CLI interfaces only. For information on managing the unit via the CLI, see the *Tsunami MP.11/QB.11 Reference Manual*.

2 Installation and Initialization

This chapter describes the steps required to install and mount the 5054, including aligning the antenna. The installation procedure does not include the mounting and connection of antennas. See the *Tsunami MP.11 Antenna Installation Guide* for this information.

If you are already familiar with this type of product, you can use the *Quick Install Guide* for streamlined installation procedures.

See the following sections:

- Hardware Overview
- Product Package
- Installation Procedure
  - Step 1: Choose a Location
  - Step 2: Unpack Shipping Box
  - Step 3: Attach Base (for Desktop or Ceiling Mounting only)
  - Step 4: Remove Covers
  - Step 5: Connect the Cables
  - Step 6: Mount the Unit
  - Step 7: Power on the Unit
  - Step 8: View LEDs
  - Step 9: Align the Antenna
  - Step 10: Attach Kensington Security Lock (Optional)
  - Step 11: Install Documentation and Software
- Initialization
  - ScanTool
  - Setting the IP Address with ScanTool
- Logging in to the Web Interface

Hardware Overview

The 5054 supports two power methods: an AC power outlet and Power-over-Ethernet. The power supply accepts an input AC voltage in the range of 100-240 VAC.

Power-over-Ethernet

The unit is equipped with a Power-over-Ethernet (PoE) module. Using PoE, you can provide electricity and wired connectivity to the unit over a single Category 5 cable. If you use PoE, there is no difference in operation; the only difference is the power source.

- The PoE integrated module provides -48 VDC over a standard CAT5 Ethernet cable.
- Maximum power supplied to the 5054 is 11 Watts. The units typically draw less than 7.5 Watts.
- You must have an PoE hub (also known as a power injector) connected to the network to use Power-over-Ethernet. The PoE hub is not a repeater and does not amplify the Ethernet data signal.
- If connected to a PoE hub and an AC power supply simultaneously, the radio draws power from PoE.
- The cable length between the PoE hub and the radio should not exceed 100 meters (approximately 325 feet).

Product Package

Each shipment includes the items in the following table. Verify that you have received all parts of the shipment.

NOTE: *Unless noted in this table, cables are not supplied with the unit.*

Tsunami MP.11 5054 (MP.11a) unit	
Power Adaptor	
Mounting Stand	
Mounting Hardware	**Quantity** **Description** 4 ea. Mounting Plug (6 mm x 40 mm) 4 ea. Pan-head Screw (3.5 mm x 40 mm)
Installation CD and Quick Installation Guide	

<table>
<tr><td>15 dBi Window Antenna (included with 5054-RSU-xx-WA; available for order separately)</td><td> </td></tr>
<tr><td>Outdoor Antenna Mounting Hardware and Documentation (included with 5054-RSU-xx-WA)</td><td><u>Quantity</u> <u>Description</u>
2 ea L-Type Mounting Plate (top)
2 ea L-Type Mounting Plate (bottom)
6 ea. M5 Screw (with washer)
2 ea Screw
2 ea. Wall Mounting Plug (Wall-Tiger)
1 ea. Outdoor Mounting Configuration Flyer</td></tr>
<tr><td>Indoor Antenna Mounting Hardware and Documentation (included with 5054-RSU-xx-WA)</td><td><u>Quantity</u> <u>Description</u>
2 ea Screw
2 ea Washer
2 ea. Suction Cup/Rotation Bar
1 ea. Indoor Mounting Configuration Flyer</td></tr>
</table>

Installation Procedure

IMPORTANT:
Before installing and using this product, see Safety and Regulatory Compliance Information on the product CD.

IMPORTANT:
All units must be installed by a suitably trained professional installation technician or by a qualified installation service.

WARNING:
For your own safety, when using DC power, use only the power adaptor supplied with the unit.

WARNING:
The metal case of the unit must be grounded through the ground connection that is provided on the metal case. The antenna grounding, the surge arrestor, and the 5054 unit housing must be bonded together and grounded in one location to avoid ground current loops.

NOTES:

- *The **Configure System** window provides a selectable **Country** field that automatically provides the allowed bandwidth and frequencies for the selected country as well as, where applicable, Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC).*
- *Non-US installers should not add an antenna system until the **Country** is selected, the unit is rebooted, and the proper power level is configured.*
- *Be sure to read the **Release Notes** file on the product CD as it contains software version and driver information that may not have been available when this document was produced.*
- *When using PoE, use only a power injector that meets these requirements:*
  - *UL-Listed/ITE (NWGQ)*
  - *Limited Power Source Output per UL/IEC 60950*
  - *CE-marked*
  - *Approved for Power-over-Ethernet*
  - *Rated output, 48 Vdc/0.42 A*
  - *Pinout follows 802.3af standard for mid-span devices*

The following installation procedure provides instructions for attaching both the power and Ethernet connectors. In situations without an external antenna (for example, during a desk tryout), the antenna cable is not required.

See the following steps:

- Step 1: Choose a Location

- Step 2: Unpack Shipping Box
- Step 3: Attach Base (for Desktop or Ceiling Mounting only)
- Step 4: Remove Covers
- Step 5: Connect the Cables
- Step 6: Mount the Unit
- Step 7: Power on the Unit
- Step 8: View LEDs
- Step 9: Align the Antenna
- Step 10: Attach Kensington Security Lock (Optional)
- Step 11: Install Documentation and Software

Step 1: Choose a Location

To make optimal use of the 5054, you must find a suitable location for the hardware. The range of the unit largely depends upon the position of the antenna. Proxim recommends you do a site survey, observing the following requirements, before mounting the 5054 hardware.

- The location must allow easy disconnection of the unit from the power outlet if necessary.
- The unit must not be covered and the air must be able to flow freely around the unit.
- The unit must be kept away from vibration, excessive heat, and humidity, and kept free from dust buildup.
- The installation must conform to local regulations at all times.

CAUTION: *Proxim recommends the use of a lightning arrestor at the building ingress point. You can purchase the Proxim Lightning Protector; see the documentation that comes with the Lightning Protector for more information and installation instructions.*

Step 2: Unpack Shipping Box

1. Unpack the unit and accessories from the shipping box.
2. Note the Ethernet and MAC addresses of the unit, as well as the serial number; these addresses may be used when configuring the unit.

   NOTE: *The serial number is required to obtain support from Proxim. Keep this information in a safe place.*

Step 3: Attach Base (for Desktop or Ceiling Mounting only)

If the unit will be mounted on a desktop or to a ceiling, attach the metal base as follows. If the unit will be mounted to a wall, proceed to Step 4: Remove Covers.

1. Insert the posts in the metal base into the holes on the bottom of the 5054 unit.

2. Using a Phillips-head screwdriver, tighten the screws on the bottom of the metal base to securely attach the base to the unit.

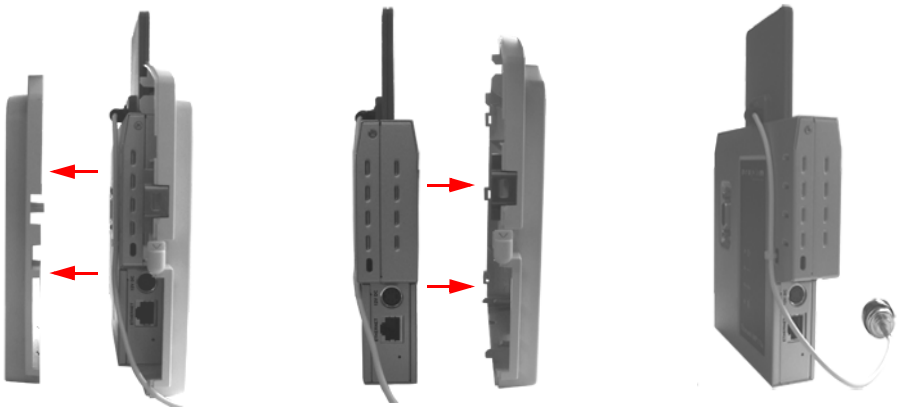
Step 4: Remove Covers

In order to cable the unit for operation, you must first remove the front, back, and cable covers.

1. Unlock the unit's cable cover by pressing down on the cable cover lock located on the side of the unit.

2. Pull the thin arm of the cable cover away from the unit and upward to remove the cable cover.

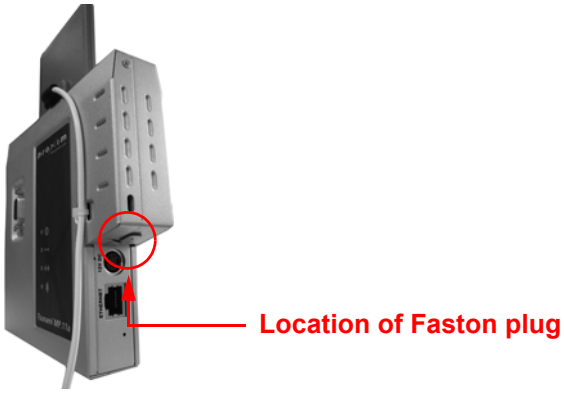
3. Remove the front cover from the unit (the side with the LED indicators, shown in figure **A**); then remove the back cover (figure **B**). The unit with all covers removed is shown in figure **C**.



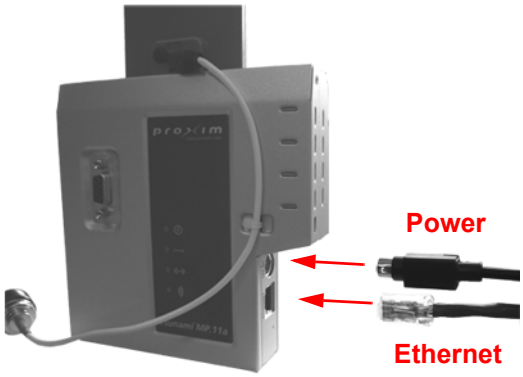
A **B** **C**

Step 5: Connect the Cables

1. Identify the location at which you intend to mount the unit.
2. Connect the grounding wire to the 5054 using the Faston plug on the metal case, next to the power plug.



3. Connect one end of an Ethernet cable to the Ethernet port.
   - If you intend to connect the 5054 to a hub, switch, patch panel, or PoE power injector, use a straight-through Ethernet cable.
   - If you intend to connect the 5054 to a single computer, use a cross-over Ethernet cable.
4. If you are not using Active Ethernet, or you want to connect the 5054 to Active Ethernet and AC power simultaneously, attach the AC power cable to the unit's power port.



Step 6: Mount the Unit

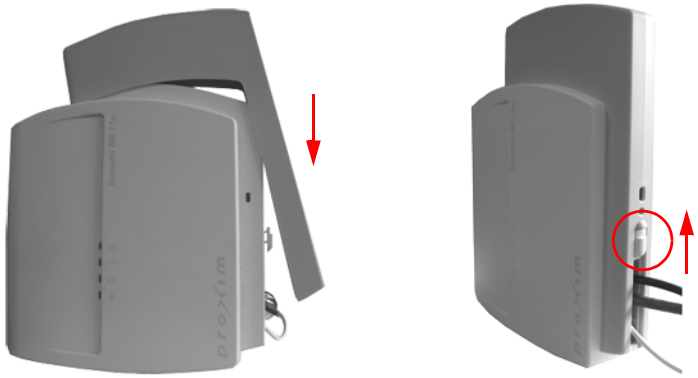
- Desktop Mount
- Wall Mount
- Ceiling Mount

Desktop Mount

1. Fit the radio inside the back cover, with the serial connection and LED indicators facing out.

2. Replace the front cover, threading the cables through the opening at the lower right side of the cover.

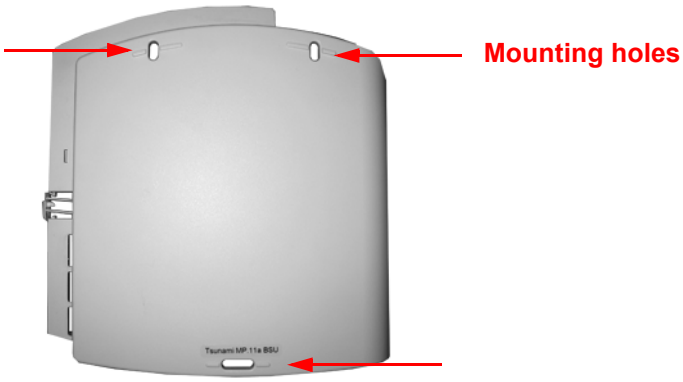
3. Replace the cable cover (figure A), ensuring that the release latch clicks upwards to the closed position (figure B).



4. If you have not done so before, attach the metal base as described in Step 3: Attach Base (for Desktop or Ceiling Mounting only).

Wall Mount

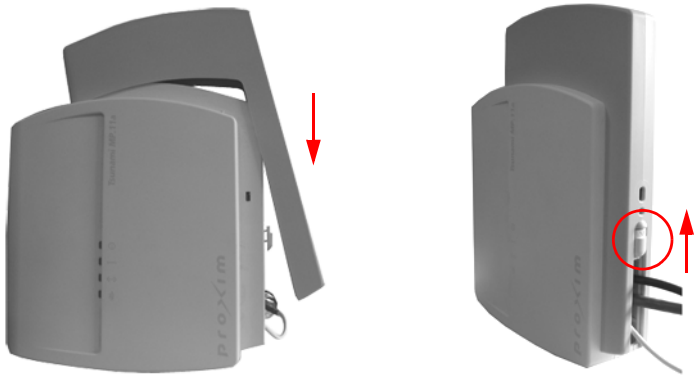
1. Place the back cover on the mounting location and mark the center of the three mounting holes.



2. Remove the cover from the wall and drill a hole at each of the locations you marked. Each hole should be wide enough to hold a mounting plug (6 mm x 35 mm).
3. Insert a plug into each hole. (Four 6 mm x 35 mm plugs are provided; you need to use only three of these for wall mounting.)
4. Insert a screw into each of the mounting holes molded into the back cover, and align with the holes on the wall. (Four 3.5 mm x 40 mm pan-head screws are provided; you need to use only three of these for wall mounting.)
5. Use a screwdriver to tighten the screws, attaching the back cover to the wall.
6. Fit the radio inside the back cover, with the serial connection and LED indicators facing out.

7. Replace the front cover, threading the cables through the opening at the lower right side of the cover.

8. Replace the cable cover (figure A), ensuring that the release latch clicks upwards to the closed position (figure B).

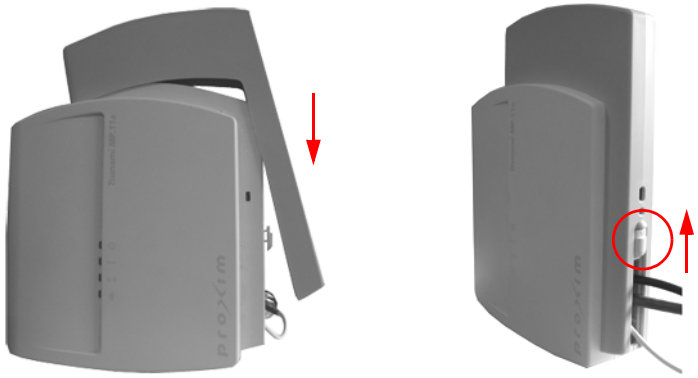


Ceiling Mount

1. Fit the radio inside the back cover, with the serial connection and LED indicators facing out.

2. Replace the front cover, threading the cables through the opening at the lower right side of the cover.

3. Replace the cable cover (figure **A**), ensuring that the release latch clicks upwards to the closed position (figure **B**).



4. If you have not done so before, attach the metal base as described in Step 3: Attach Base (for Desktop or Ceiling Mounting only).
5. Feed a mounting screw through each of the four rubber feet. The 5054 comes with four 3.5 mm x 40 mm pan-head screws.

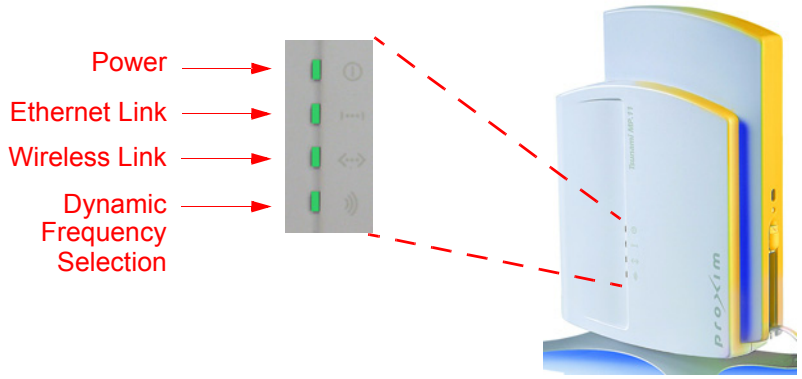
6. Remove the screws from the rubber feet.
7. With the 5054 turned upside down, position the base against the ceiling where you want to mount the unit.
8. Mark the center of the four mounting holes in the rubber feet.
9. Set the 5054 aside and drill a hole at each of the locations you marked. Each hole should be wide enough to hold a mounting plug (6 mm x 35 mm).
10. Insert a plug into each hole. The 5054 comes with four 6 mm x 35 mm plugs.
11. Insert the screws into the holes you made previously in the rubber feet.
12. Insert the screws into the mounting plugs.
13. Use a screwdriver to tighten the screws, attaching the 5054's metal base to the ceiling.

Step 7: Power on the Unit

The 5054 can be powered by a power supply (just plug the power cord of the power supply into an AC power outlet), or by PoE (connect a PoE splitter to the Ethernet cabling).

Step 8: View LEDs

When the unit is powered on, the 5054 performs startup diagnostics. When startup is completed, the LEDs show the operational state of the 5054 (see the following figure).



The following table shows the status of the LEDs when the 5054 is operational (the fourth LED is only used during Dynamic Frequency Selection on a BSU).

LED	Power	Ethernet Link	Wireless Link	Dynamic Frequency Selection
Off	Power is not present or is malfunctioning.	Not connected.	Wireless interface is up properly but no wireless link established.	
Green	Power is present; the unit is operational.	Connected at 10 Mbps.	Immediately after connecting a wireless link.	
Blinking Green	N/A	Data is being sent at 10 Mbps.	Data is being sent or the wireless interface is initializing after reboot (less than two minutes).	Scanning for channel.
Amber	The unit is initializing after reboot (less than two minutes); it cannot get a dynamic IP address.	Connected at 100 Mbps, or the unit is initializing after reboot (less than two minutes).	N/A	N/A
Blinking Amber	N/A	Data is being sent at 100 Mbps.	N/A	N/A
Red	A fatal error in the unit.	An error in data transfer.	There is a fatal error on the wireless interface.	N/A

Step 9: Align the Antenna

Antenna alignment is the process of physically aligning the antenna of the radio receiver and transmitter to have the best possible link established between them. The antenna alignment process is usually performed during installation and after major repairs.

Antenna Alignment Display (AAD) provides a measurement of signal quality in an easy-to-interpret manner—a numeric printed signal value at the CLI and serial ports. The SNR is numerically displayed on the CLI or serial port by two decimal characters representing a number from 00 to 99. On the serial port, AAD is enabled by default after booting.

To start the display, you must enable AAD and a wireless link must be established between the BSU and the SU.

Aiming is complete if moving in any direction results in a falling SNR value.

NOTES:

- *Antenna alignment for the Base Station is useful only for a point-to-point link.*
- *The Antenna Alignment Display (AAD) CLI command is disabled automatically 30 minutes after it is enabled to remove the load of extra messages on the wireless interface. The default telnet timeout is 900 seconds (15 minutes). If AAD must run for the entire 30 minutes, change the default telnet timeout value to a value greater than 30 minutes (greater than 1800 seconds). This restriction is for telnet connections only and not for the serial interface. The serial interface never times out; however, the AAD command does still time out.*

Antenna Alignment Commands

- **`set aad enable local`**: Enables display of the local SNR. Local SNR is the SNR measured by the receiver at the near end.
- **`set aad enable remote`**: Enables display of the remote SNR. Remote SNR is the SNR as measured by the receiver at the far end.
- **`set aad enable average`**: Enables display of the average SNR. The average SNR is the average of the local and remote SNR.
- **`set aad disable`**: Disables Antenna Alignment Display (Ctrl-C also disables AAD).

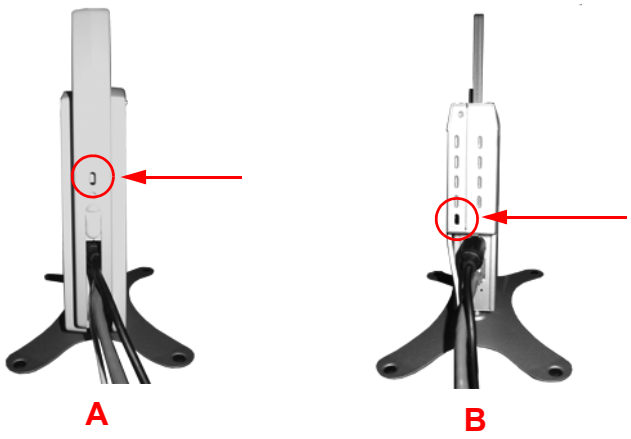
Step 10: Attach Kensington Security Lock (Optional)

If desired, you can attach a Kensington lock to secure the cable cover into place. This protects the unit from unauthorized tampering.

The 5054 enclosure includes a Kensington Security Slot for use with a Kensington locking mechanism. When properly installed, a Kensington lock can prevent unauthorized personnel from stealing the 5054. In addition, the Kensington lock secures the cable cover in place, which prevents tampering with the Ethernet and power cables.

The Kensington Security Slot is shown in the following figures. Figure A shows the slot with the unit's covers attached; figure B shows the slot with the unit's covers removed).

For information about Kensington security solutions, go to http://www.kensington.com.



Step 11: Install Documentation and Software

To install the documentation and software on a computer or network:

1. Place the CD in a CD-ROM drive. The installer normally starts automatically. (If the installation program does not start automatically, click **setup.exe** on the installation CD.)
2. Click the Install Software and Documentation button and follow the instructions displayed on the installer windows. The following documentation and software products are installed:
   - Available from **Start > All Programs > Tsunami > MP.11 5054**:
     - Documentation (in **Docs** subdirectory):
       - Installation and Management Guide
       - Quick Installation Guide
       - Reference Manual
       - Safety and Regulatory Guide
       - Recommended Antenna Guide
       - Antenna Installation Guide
     - Online Help
     - Scan Tool (in **Scan Tool** subdirectory)
     - TFTP Server (in **TFTP Server** subdirectory)

     NOTE: *All of these items are also available from* ***C:\Program Files\Tsunami\MP.11 5054****.*
   - Available from **C:\Program Files\Tsunami\MP.11 5054**:
     - Documentation (in **Docs** folder): See list above
     - Help files (in **Help** folder; click on index.htm to access)
     - TFTP Server and Scan Tool program (in **Extras** folder)
     - MIBs (in **MIBs** folder)

Initialization

Connecting to the unit requires either:

- A direct physical connection with an Ethernet cross-over cable or with a serial RS232C cable
- A network connection

Connecting with a serial connection, allows you to configure and manage the unit with the CLI. Connecting with the other connections allows you to use of the Web Interface and SNMP in addition to the CLI.

Using a serial connection, you can access the unit through a terminal emulation program such as HyperTerminal. (See "HyperTerminal Connection Properties" in the *Tsunami MP.11/QB.11 Reference Manual*.)

For all other modes of connection, you will need the IP address of the unit in order to use the Web Interface, SNMP, or the CLI. Because each network is different, an IP address suitable for your network must be assigned to the unit. You must know this IP address to configure and manage the unit through its Web Interface, SNMP, or the CLI. The unit can use either a **static** or **dynamic** IP address. The unit either obtains its IP address automatically through DHCP (dynamic IP address) or it must be set manually (static IP address).

ScanTool

With ScanTool (a software utility that is included on the product installation CD), you can find out the current IP address of the unit and, if necessary, change it so that is appropriate for your network. The units are shipped with the static IP address 10.0.0.1 configured.

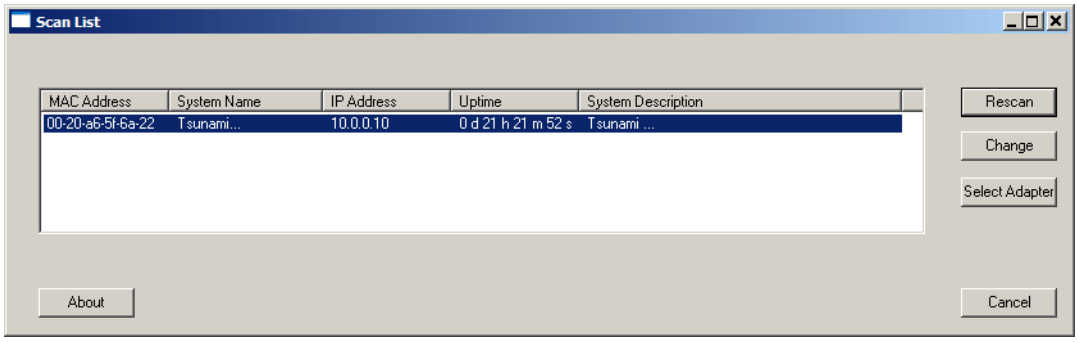
ScanTool lets you find the IP address of a Tsunami MP.11 by referencing the MAC address in a Scan List, or to assign an IP address if the correct one has not been assigned. The tool automatically detects the units installed on your network segment, regardless of IP address, and lets you configure each unit's IP settings. In addition, you can use ScanTool to download new software to a unit that does not have a valid software image installed.

Setting the IP Address with ScanTool

To discover and set/change the IP address of the unit:

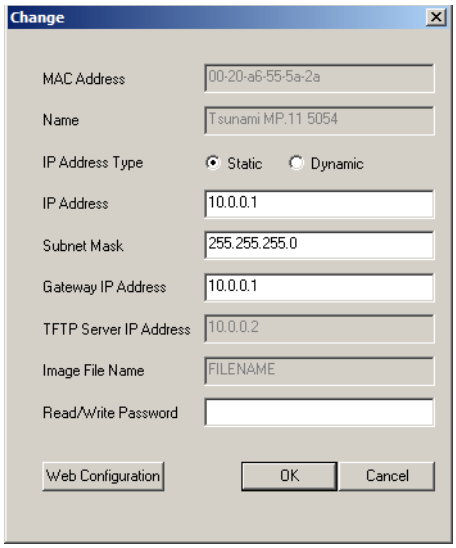
1. Run ScanTool on a computer connected to the same LAN subnet as the unit, or a computer directly connected to the unit with a cross-over Ethernet cable. Double-click the **ScanTool** icon on the Windows desktop to launch the program. If the icon is not on your desktop, click **Start** > **All Programs** > **Tsunami** > **MP.11 5054** > **Scan Tool**.

   ScanTool scans the subnet for the unit and displays a list of the units it finds in the Scan List window (shown below). If necessary, click **Rescan** to re-scan the subnet and update the display.



   You can assign a new IP address to one unit, even if more than one unit has the same (default) IP address 10.0.0.1, but the new IP address must be unique to allow use of the management interfaces.

2. Select the unit for which you want to set the IP address and click **Change**. The **Change** dialog window is displayed, as shown below.



3. To set the IP address ***manually***, ensure that **Static** is selected as the **IP Address Type** and fill in the **IP Address** and **Subnet Mask** suitable for the LAN subnet to which the unit is connected.

   To set the IP address ***dynamically***, ensure that **Dynamic** is selected as the **IP Address Type**. The unit will request its IP address from a DHCP server on your network.

4. Enter the **Read/Write Password** (the default value is **public**) and click **OK** to confirm your changes. The respective unit reboots to make the changes effective.

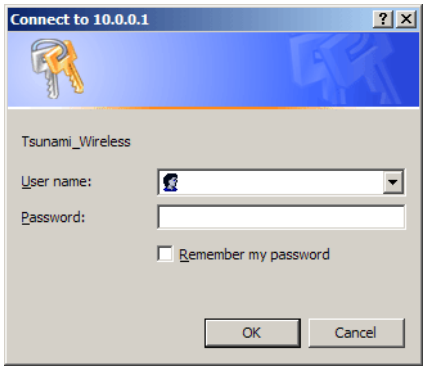
Logging in to the Web Interface

The Web Interface provides a graphical user interface through which you can easily configure and manage the unit. This section describes only how to access the Web Interface.

To use the Web Interface, you need only the IP address of the unit. (See Setting the IP Address with ScanTool for details).

NOTE: *If the connection is slow or you are not able to connect, use the Internet Explorer Tools option to ensure you are not using a proxy server for the connection with your Web browser.*

To access the unit with a Web browser, start your Web browser and enter the IP address of the unit. The Web address must appear as **http://<ip address>** (for example, **http://10.0.0.1**). A window such as the following is displayed.



Do not fill in the **User Name**; enter only the password and click **OK**. The default password is **public**.

The **System Status** window is displayed. To find out more about the information presented in this window, see the Status chapter.

You now have access to the unit's Web Interface. The remainder of this manual describes configuring and monitoring the unit using this interface.

3 System Overview

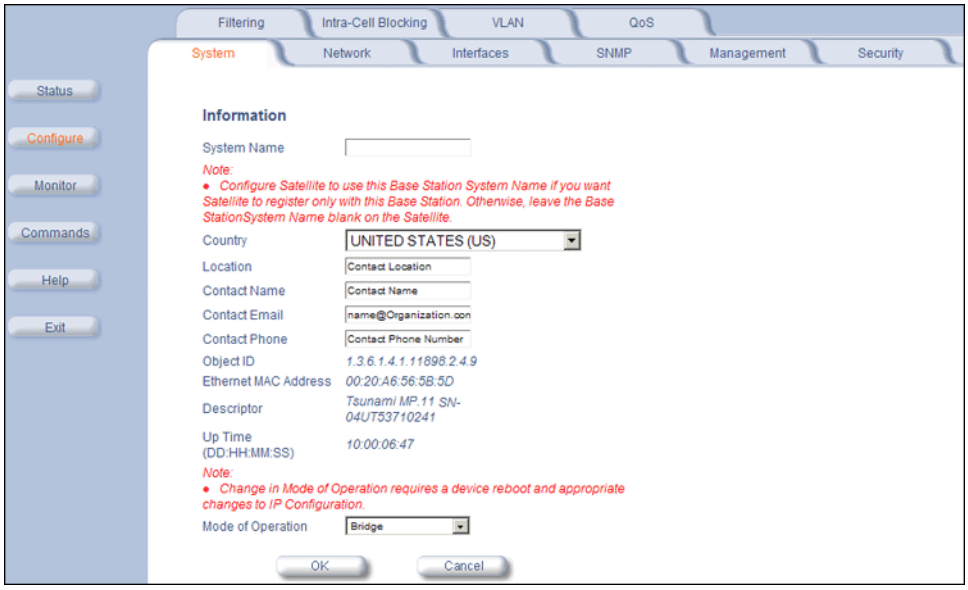
This chapter provides an overview of the system. See the following sections:

- Changing Basic Configuration Information
  - Country and Related Settings
  - Dynamic Frequency Selection (DFS)
  - Transmit Power Control
- SU Registration
- Dynamic Data Rate Selection (DDRS)
- Virtual Local Area Networks (VLANs)
- Quality of Service (QoS)
  - Concepts and Definitions

Changing Basic Configuration Information

To view or change basic system information, click the **Configure** button on the left side of the Web interface window, then click the **System** tab. See System Parameters for detailed information about the fields and selections in this window.

NOTE: *System Name by default contains the actual model number. The following screenshot is for information only.*



Country and Related Settings

The unit's **Configure System** window provides a selectable **Country** field that automatically provides the allowed bandwidth and frequencies for the selected country and band.

Units sold only in the United States are pre-configured to scan and display only the outdoor frequencies permitted by the FCC. No other **Country** can be configured. Units sold outside of the United States support the selection of a **Country** by the professional installer.

NOTE: *Non-US installers should not add an antenna system until the **Country** is selected, the unit is rebooted, and the proper power level is configured. The output power level of the final channel selected by DFS scan can be found in the Event Log.*

The Dynamic Frequency Selection (DFS) feature is enabled automatically when you choose a country and band that require it. The Transmit Power Control (TPC) feature is always available.

Click **Configure** > **System**; then select the appropriate country and band for your regulatory domain from the **Country** drop-down box.

Continue configuring settings as desired; then click **Commands** > **Reboot** to save and activate the settings. Alternatively, if you want to save the configuration settings to the flash memory but not activate the settings, use the **save config** CLI command.

Dynamic Frequency Selection (DFS)

The Tsunami MP.11 5054 supports Dynamic Frequency Selection (DFS) for FCC, IC, and ETSI regulatory domains per FCC Part 15 Rules for U-NII devices, IC RSS-210, and ETSI EN 301-893 and 302-502 regulations, respectively. These rules and regulations require that 802.11a devices use DFS to prevent interference with radar systems and other devices that already occupy the 5 GHz band.

During boot-up, the unit scans the available frequency and selects the best channel. If the unit subsequently detects interference on its channel, it rescans to find a better channel. Upon finding a new channel, the unit is required to wait 60 seconds to ensure that the channel is not busy or occupied by radar, and then commences normal operation. (In Canada, if the channel was previously blacklisted, the unit scans for 600 seconds before commencing normal operation if the selected channel frequency is in the 5600 - 5650 MHz range).

If you are using the unit in a country and band that require DFS, keep in mind the following:

- DFS is not a configurable parameter; it is always enabled and cannot be disabled.
- You cannot manually select the device's operating channel; you must let the unit select the channel. You may make channels unavailable by manually "blacklisting" them and preventing those channels being selected, in accordance with local regulations or interference. You can also display the Channel Blacklist Table to view the channels that have been blacklisted.
- In compliance with FCC regulations, the unit uses ATPC (Automatic Transmit Power Control) to automatically adapt transmit power when the quality of the link is more than sufficient to maintain a good communication with reduced transmit power. See Transmit Power Control for more information.

Dynamic Frequency Selection (DFS) is enabled automatically based upon the country and band you select. You can tell DFS is in use because the **Frequency Channel** field on the **Interfaces** page displays only the DFS-selected frequency. DFS scans all available frequencies, starting with the DFS preferred channel (when configured) and skipping blacklisted channels, to select the operating frequency automatically.

A country/band selection with DFS enabled causes the Base Station to come up in scan mode. It scans the available frequencies and channels to avoid radar and selects a channel with the least interference.

NOTE: *Scanning is performed only on the frequencies allowed in the regulatory domain of the country and band selected when it is required for radar detection and avoidance.*

The SU also comes up in scan mode to scan all available frequencies to find a BSU with which it can register. Scanning may take several minutes. After establishing a wireless link, the wireless LED stops flashing and continues to shine green.

NOTE: *Because DFS may need to scan for radar on multiple channels, you must allow a sufficient amount of time for the units to start up. This is considerably longer than when the unit is not using DFS. This is expected behavior. Startup time is within four minutes if no radar is detected, but up to one minute is added for every selected channel that results in radar detection.*

DFS is required for three purposes:

1. *Radar avoidance both at startup and while operational*. To meet these requirements, the BSU scans available frequencies at startup. If a DFS-enabled channel is busy or occupied with radar, the system will blacklist the channel for a period of 30 minutes in accordance with FCC, IC, and ETSI regulations. Once fully operational on a frequency, the BSU actively monitors the occupied frequency. If interference is detected, the BSU blacklists the channel, logs a message and rescans to find a new frequency that is not busy and is free of radar interference.

   Radar detection is performed only by the BSU and not by the SU. When an SU is set to a country/band in which DFS is used, it scans all available channels upon startup looking for a BSU that best matches its connection criteria (such as **Base Station System Name**, **Network Name**, and **Shared Secret**). The SU connects to the BSU automatically on whatever frequency the BSU has selected. Because of this procedure, it is best to set up the BSU and have it fully operational before installing the SU, although this is not required. If a BSU rescans because of radar interference, the SU loses its wireless link. The SU waits 30 seconds (when the Mobility feature is enabled, the SU starts scanning for a BSU instantly rather than waiting 30 seconds); if it finds that it could not receive the BSU in this amount of time, it rescans the available frequencies for an available BSU.
2. *Guarantee the efficient use of available frequencies by all devices in a certain area*. To meet this requirement, the BSU scans each available frequency upon startup and selects a frequency based upon the least amount of noise and interference detected. This lets multiple devices operate in the same area with limited interference. This procedure is done only at startup; if another UNII device comes up on the same frequency, the BSU does not detect this or rescan because of it. It is expected that other devices using these frequencies also are in compliance with country/band regulations, so this should not happen.
3. *Uniform Channel Spreading.* To meet this requirement, the MP.11 5054 randomly selects operating channel from the available channels with least interference. If the DFS Preferred Channel is configured, the unit begins by scanning that channel. If no interference is detected, the unit makes this channel operational. If the channel is busy or occupied by radar, the unit blacklists that channel and scans other available channels for the one with least interference. This implements the Uniform Channel Spreading requirement by either automatically selecting the channel with least interference or allowing the installer to manually select a channel with least interference from a channel plan.

Transmit Power Control

Transmit Power Control is a manual configuration selection to reduce the unit's output power. The maximum output power level for the operating frequency can be found in the event log of the unit's embedded software.

ATPC (Automatic Transmit Power Control) is a feature to automatically adapt transmit power when the quality of the link is more than sufficient to maintain a good communication with reduced transmit power. This feature is required for FCC DFS. It works by monitoring the quality of the link and reducing the output power of the radio by up to 6 dB when good link quality can still be achieved. When link quality reduces, the output power is automatically increased up to the original power level to maintain a good link. For a full discussion of DFS, see Dynamic Data Rate Selection (DDRS) above.

By default, the unit lets you transmit at the maximum output power that the radio can sustain for data rate and frequency selected. However, with Transmit Power Control (TPC), you can adjust the output power of the unit to a lower level in order to reduce interference to neighboring devices or to use a higher gain antenna without violating the maximum radiated output power allowed for your country and band. Also, some countries that require DFS also require the transmit power to be set to a 6 dB lower value than the maximum allowed EIRP when link quality permits, as part of the DFS requirements.

NOTE: *When the system is set to transmit at the maximum power, professional installers must ensure that the maximum EIRP limit is not exceeded. To achieve this, they may have to add attenuation between the device and the antenna when a high gain antenna is used.*

NOTE: *You can see your unit's current output power for the selected frequency in the event log. The event log shows the selected power for all data rates, so you must look up the relevant data rate to determine the actual power level.*

NOTE: *This feature only lets you decrease your output power; you cannot increase your output power beyond the maximum the radio allows for your frequency and data rate.*

See System Parameters to configure **Country.** See Interface Parameters to configure Transmit Power Control.

SU Registration

The list of parameters you must configure for registration of the SU on a BSU are:

- Network Name
- Base Station System Name (when used; otherwise, leave blank)
- Network Secret
- Encryption (when used)
- Frequency Channel (when available)

See System Parameters to see the description of these fields and to configure them.

NOTES:

- *The frequency channel must be the same for the BSU and the SU in order to register the SU when roaming is not enabled and DFS is not required.*
- *Channel Bandwidth and Turbo mode (when available) must be the same for the BSU and SU in order to register the SU.*
- *Roaming will automatically select a channel on the SU corresponding to the BSU channel. Roaming is the procedure in which an SU terminates the session with the current BSU and starts the registration procedure with another BSU when it finds the quality of the other BSU to be better.*

Dynamic Data Rate Selection (DDRS)

The WORP Dynamic Data Rate Selection (DDRS) lets the BSU and SUs monitor the remote average signal-to-noise ratio (SNR) and the number of retransmissions between the BSU and SUs and adjust the transmission data rate to an optimal value to provide the best possible throughput according to the current communication conditions and link quality. With DDRS enabled, a BSU can maintain different transmission data rates to different SUs, optimizing the data rate based on the link quality of each SU independently.

Both the BSU and the SUs monitor the remote SNR and number of retransmissions. The BSU monitors these values for each SU that is registered. An SU monitors these values for the BSU. When necessary, based on this information, the data rate is dynamically adjusted.

Note that DDRS is enabled or disabled on the BSU only. This operation requires the BSU to be rebooted. After rebooting, the BSU sends a multicast announcement to all SUs to begin the registration process. During registration, an SU is informed by the BSU whether DDRS is enabled or disabled and it sets its DDRS status accordingly.

See Interface Parameters to configure DDRS.

Virtual Local Area Networks (VLANs)

Virtual Local Area Networks (VLANs) are logical groupings of network hosts. Defined by software settings, other VLAN members or resources appear (to connected hosts) to be on the same physical segment, no matter where they are attached on the logical LAN or WAN segment. They simplify allowing traffic to flow between hosts and their frequently-used or restricted resources according to the VLAN configuration.

Tsunami MP.11 5054 units are fully VLAN-ready; however, by default, VLAN support is disabled. Before enabling VLAN support, certain network settings should be configured and network resources such as VLAN-aware switches should be available, dependent upon the type of configuration.

VLANs are used to conveniently, efficiently, and easily manage your network in the following ways:

- Manage VLAN configuration from a single window
- Define groups
- Reduce broadcast and multicast traffic to unnecessary destinations
  - Improve network performance and reduce latency
- Increase security
  - Secure network restricts members to resources on their own VLAN

VLAN tagged data is collected and distributed through a unit's Ethernet interface. The units can communicate across a VLAN-capable switch that analyzes VLAN-tagged packet headers and directs traffic to the appropriate ports when the units are working in their Transparent mode.

VLAN features can be managed via:

- The BSU's Web interface
- The Command Line Interface (see "Command Line Interface" in the *Tsunami MP.11/QB.11 Reference Manual*)
- SNMP (see the MIBs provided on the product CD)

For more information about VLAN configuration, see VLAN Parameters (BSU Only; Bridge Mode Only).

Quality of Service (QoS)

The Quality of Service (QoS) feature is based on the 802.16 standard and defines the classes, service flows, and packet identification rules for specific types of traffic. QoS main priority is to guarantee a reliable and adequate transmission quality for all types of traffic under conditions of high congestion and bandwidth over-subscription.

Concepts and Definitions

The software supports QoS provisioning from the BSU only. You may define different classes of service on a BSU that can then be assigned to the SUs that are associated, or that may get associated, with that BSU.

The software provides the ability to create, edit, and delete classes of service that are specified by the following hierarchy of parameters:

- Packet Identification Rule (PIR) – up to 64 rules, including 17 predefined rules
- Service Flow class (SFC) – up to 32 SFs, including 7 predefined SFCs; up to 8 PIRs may be associated per SFC
- Priority for each rule within each SF class – 0 to 255, with 0 being lowest priority
- QoS class – up to 8 QoS classes, including 4 predefined classes; up to 4 SFCs may be associated per QoS class

Packet Identification Rule (PIR)

A Packet Identification Rule is a combination of parameters that specifies what type of traffic is allowed or disallowed. The software allows the creation of up to 64 different PIRs, including 17 predefined PIRs. It provides the ability to create, edit, and delete PIRs that contain none, one, or more of the following classification fields:

- Rule Name
- IP ToS (Layer 3 QoS identification)
- IP Protocol List containing up to 4 IP protocols
- 802.1p tag (layer 2 QoS identification)
- Up to 4 pairs of Source IP address + Mask
- Up to 4 pairs of Destination IP address + Mask
- Up to 4 source TCP/UDP port ranges
- Up to 4 destination TCP/UDP port ranges
- Up to 4 source MAC addresses
- Up to 4 destination MAC addresses
- VLAN ID
- Ether type (Ethernet protocol identification)

Good examples are provided by the 17 predefined PIRs. Note that these rules help to identify specific traffic types:

1. All – No classification fields, all traffic matches
2. Cisco VoIP UL
   a. Protocol Source Port Range (16,000-32,000)
   b. IP Protocol List (17 = UDP)
3. Vonage VoIP UL
   a. Protocol Source Port Range (8000-8001, 10000-20000)
   b. IP Protocol List (17 = UDP)
4. Cisco VoIP DL
   a. Protocol Destination Port Range (16,000-32,000)
   b. IP Protocol List (17 = UDP)
5. Vonage VoIP DL

   a. Protocol Destination Port Range (8000-8001, 10000-20000)
   b. IP Protocol List (17 = UDP)
6. TCP
   a. IP Protocol List (6)
7. UDP
   a. IP Protocol List (17)
8. PPPoE Control
   a. Ethertype (type 1, 0x8863)
9. PPPoE Data
   a. Ethertype (type 1, 0x8864)
10. IP
   a. Ethertype (type 1, 0x800)
11. ARP
   a. Ethertype (type 1, 0x806)
12. Expedited Forwarding
   a. IP TOS/DSCP (low=0x2D, high=0x2D, mask = 0x3F)
13. Streaming Video (IP/TV)
   a. IP TOS/DSCP (low=0x0D, high=0x0D, mask = 0x3F)
14. 802.1p BE
   a. Ethernet Priority (low=0, high=0) (this is the equivalent of the User Priority value in the TCI (Tag Control Information) field of a VLAN tag)
15. 802.1p Voice
   a. Ethernet Priority (low=6, high=6) (this is the equivalent of the User Priority value in the TCI (Tag Control Information) field of a VLAN tag)
16. 802.1p Video
   a. Ethernet Priority (low=5, high=5) (this is the equivalent of the User Priority value in the TCI (Tag Control Information) field of a VLAN tag)
17. L2 Broadcast/Multicast
   a. Ethernet Destination (dest = 0x80000000, mask = 0x80000000)

Note that two different VoIP rule names have been defined for each direction of traffic, Uplink (UL) and Downlink (DL), (index numbers 2 to 5). This has been done to distinguish the proprietary nature of the Cisco VoIP implementation as opposed to the more standard Session Initiation Protocol (SIP) signaling found, for example, in the Vonage-type VoIP service.

Service Flow Class (SFC)

A Service Flow class defines a set of parameters that determines how a stream of application data that matches a certain classification profile will be handled. The software allows the creation of up to 32 different SFs, including seven predefined SFs. The software provides the ability to create, edit, and delete SFs that contain the following parameters and values:

- Service flow name
- Scheduling type – Best Effort (BE); Real-Time Polling Service (RtPS)
- Service Flow Direction – Downlink (DL: traffic from BSU to SU); Uplink (UL: traffic from SU to BSU)
- Maximum sustained data rate (or Maximum Information Rate, MIR) – specified in units of 1 Kbps from 8 Kbps up to he maximum rate of 108000 Kbps per SU

- Minimum reserved traffic rate (or Committed Information Rate, CIR) – specified in units of 1 Kbps from 0 Kbps up to the maximum rate of 10000 Kbps per SU
- Maximum Latency – specified in increments of 5 ms steps from a minimum of 5 ms up to a maximum of 100 ms
- Tolerable Jitter – specified in increments of 5 ms steps from a minimum of 0 ms up to the Maximum Latency (in ms)
- Traffic priority – zero (0) to seven (7), 0 being the lowest, 7 being the highest
- Maximum number of data messages in a burst – one (1) to four (4), which affects the percentage of the maximum throughput of the system
- Activation state – Active; Inactive

Note that traffic priority refers to the prioritization of this specific Service Flow.

The software tries to deliver the packets within the specified latency and jitter requirements, relative to the moment of receiving the packets in the unit. For delay-sensitive traffic the jitter must be equal to or less than the latency. A packet is buffered until an interval of time equal to the difference between Latency and Jitter (Latency – Jitter) has elapsed. The software will attempt to deliver the packet within a time window starting at (Latency – Jitter) until the maximum Latency time is reached. If the SFC's scheduling type is real-time polling (rtPS), and the packet is not delivered by that time, it will be discarded. This can lead to loss of packets without reaching the maximum throughput of the wireless link. For example, when the packets arrive in bursts on the Ethernet interface and the wireless interface is momentarily maxed out, then the packets at the "end" of the burst may be timed out before they can be sent.

Users are able to set up their own traffic characteristics (MIR, CIR, latency, jitter, etc.) per service flow class to meet their unique requirements. Good examples are provided by the seven predefined SFCs:

1. UL-Unlimited BE
   a. Scheduling Type = Best Effort
   b. Service Flow Direction = Uplink
   c. Initialization State = Active
   d. Maximum Sustained Data Rate = 20 Mbps
   e. Traffic Priority = 0
2. DL-Unlimited BE (same as UL-Unlimited BE, except Service Flow Direction = Downlink)
3. UL-G711 20 ms VoIP rtPS
   a. Schedule type = Real time Polling
   b. Service Flow Direction = Uplink
   c. Initialization State = Active
   d. Maximum Sustained Data Rate = 88 Kbps
   e. Minimum Reserved Traffic Rate = 88 Kbps
   f. Maximum Latency = 20 milliseconds
   g. Traffic Priority = 1
4. DL-G711 20 ms VoIP rtPS (same as UL-G711 20ms VoIP rtPS, except Service Flow Direction = Downlink)
5. UL-G729 20 ms VoIP rtPS (same as UL-G711 20ms VoIP rtPS, except Maximum Sustained Data Rate and Maximum Reserved Traffic Rate = 64 Kbps)
6. DL-G729 20 ms VoIP rtPS (same as UL-G729 20ms VoIP rtPS, except Service Flow Direction = Downlink)
7. DL-2Mbps Video
   a. Schedule type = Real time Polling
   b. Service Flow Direction = Downlink
   c. Initialization State = Active
   d. Maximum Sustained Data Rate = 2 Mbps
   e. Minimum Reserved Traffic Rate = 2 Mbps
   f. Maximum Latency = 20 milliseconds

g. Traffic Priority = 1

Note that two different VoIP Service Flow classes for each direction of traffic have been defined (index numbers 3 to 6), which follow the ITU-T standard nomenclatures: G.711 refers to a type of audio companding and encoding that produces a 64 Kbps bitstream, suitable for all types of audio signals. G.729 is appropriate for voice and VoIP applications, but cannot transport music or fax tones reliably. This type of companding and encoding produces a bitstream between 6.4 and 11.8 Kbps (typically 8 Kbps) according to the quality of voice transport that is desired.

QoS Class

A QoS class is defined by a set of parameters that includes the PIRs and SFCs that were previously configured. The software allows the creation of up to eight different QoS classes, including four predefined QoS classes. Up to four SF classes can be associated to each QoS class, and up to eight PIRs can be associated to each SF class. For example, a QoS class called “G711 VoIP” may include the following SFCs: “UL-G711 20 ms VoIP rtPS” and “DL-G711 20 ms VoIP rtPS”. In turn, the SFC named “UL-G711 20 ms VoIP rtPS” may include the following rules: “Cisco VoIP UL” and “Vonage VoIP UL”.

The software provides the ability to create, edit, and delete QoS classes that contain the following parameters:

- QoS class name
- Service Flow (SF) class name list per QoS class (up to four SF classes can be associated to each QoS class)
- Packet Identification Rule (PIR) list per SF class (up to eight PIRs can be associated to each SF class)
- Priority per rule which defines the order of execution of PIRs during packet identification process. The PIR priority is a number in the range 0-63, with priority 63 being executed first, and priority 0 being executed last. The PIR priority is defined within a QoS class, and can be different for the same PIR in some other QoS class. If all PIRs within one QoS class have the same priority, the order of execution of PIR rules will be defined by the order of definition of SFCs, and by the order of definition of PIRs in each SFC, within that QoS class.

Good examples of this hierarchy are provided by the four predefined QoS classes:

1. Unlimited Best Effort
   a. SF class: UL-Unlimited BE
      PIR: All; PIR Priority: 0
   b. SF class: DL-Unlimited BE
      PIR: All; PIR Priority: 0
2. G711 VoIP
   a. SF class: UL-G711 20 ms VoIP rtPS
      PIR: Vonage VoIP UL; PIR Priority: 1
      PIR: Cisco VoIP UL; PIR Priority: 1
   b. SF class: DL-G711 20 ms VoIP rtPS
      PIR: Vonage VoIP DL; PIR Priority: 1
      PIR: Cisco VoIP DL; PIR Priority: 1
3. G729 VoIP
   a. SF class: UL-G729 20 ms VoIP rtPS
      PIR: Vonage VoIP UL; PIR Priority: 1
      PIR: Cisco VoIP UL; PIR Priority: 1
   b. SF class: DL-G729 20 ms VoIP rtPS
      PIR: Vonage VoIP DL; PIR Priority: 1
      PIR: Cisco VoIP DL; PIR Priority: 1
4. 2Mbps Video
   a. SF class: DL-2Mbps Video
      PIR: Streaming Video (IP/TV); PIR Priority: 1

4 Basic Management

This chapter describes basic features and functionality of the unit. In most cases, configuring these basic features is sufficient. The “Glossary” in the *Tsunami MP.11/QB.11 Reference Manual* provides a brief explanation of the terms used. For CLI commands you can use for basic management, see “Command Line Interface” in the *Tsunami MP.11/QB.11 Reference Manual*.

The following topics are discussed in this chapter:

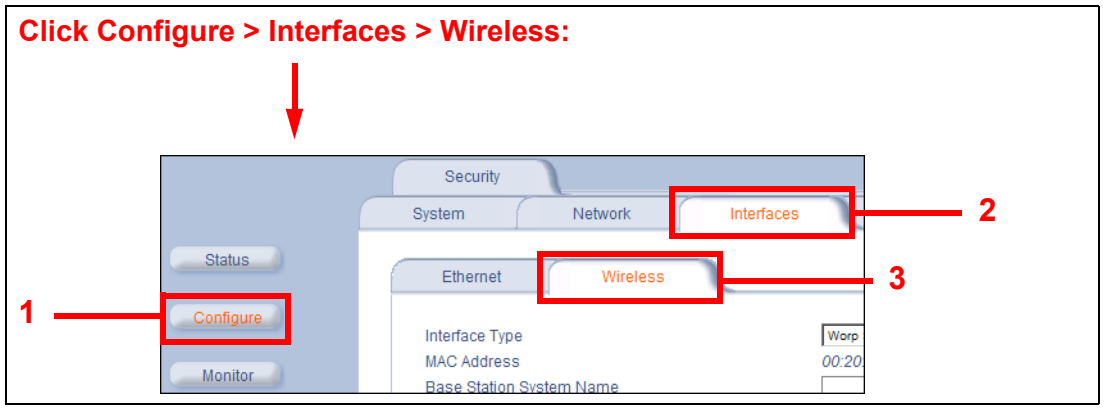
- Navigation
- Rebooting and Resetting
- General Configuration Settings
- Monitoring Settings
- Security Settings
- Default Settings
- Upgrading the Unit

Navigation

To use the Web Interface for configuration and management, you must access the unit. With ScanTool you can determine the unit’s current IP address. Then enter **http://<ip address>** in your Web browser (for example **http://10.0.0.1**). See Setting the IP Address with ScanTool for details.

NOTE: *If you have your Security Internet Options set to **High**, you may not be able to access the Web interface successfully; a high security setting disables JavaScript, which is required for running Proxim’s Web browser interface. Adding the radio’s IP address as a Trusted site should fix this problem.*

The Web Interface consists of Web page buttons and tabs. A tab can also contain sub-tabs. The following figure shows the convention used to guide you to the correct tab or sub-tab.



The Web Interface also provides online help, which is stored on your computer (see Step 11: Install Documentation and Software for details).

Rebooting and Resetting

All configuration changes require a restart unless otherwise stated. You can restart the unit with the **Reboot** command; see Rebooting, below).

Most changes you make become effective only when the unit is rebooted. A reboot stores configuration information in non-volatile memory and then restarts the unit with the new values (see Soft Reset to Factory Default).

In some cases, the unit reminds you that a reboot is required for a change to take effect. You need not reboot immediately; you can reboot after you have made all your changes.

NOTE: *Saving of the unit's configuration occurs only during a controlled reboot or by specifically issuing the CLI* ***Save*** *command. If you make changes to settings without a controlled reboot (command) and you have not issued the* ***Save*** *command, a power outage would wipe out all changes since the last reboot. For example, entering static routes takes effect immediately; however, the routes are not saved until the unit has gone through a controlled reboot. Proxim strongly recommends saving your settings immediately when you finish making changes.*

Rebooting

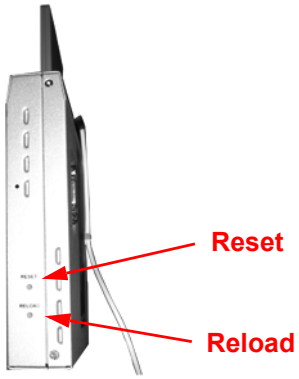
When you reboot, the changes you have made become effective and the unit is restarted. The changes are saved automatically in non-volatile memory before the actual reboot takes place.

To reboot, click **Commands** > **Reboot** > **Reboot**. The unit restarts the embedded software. During reboot, you are redirected to a page showing a countdown timer, and you are redirected to the **Status** page after the timer counts down to 0 (zero). The CLI is disconnected during reboot. This means that a new telnet session must be started.

Resetting Hardware

If the unit does not respond for some reason and you are not able to reboot, you can restart by means of a hardware reset. This restarts the hardware and embedded software. The last saved configuration is used. Any changes that you have made since then are lost.

To reset the hardware, use the end of a paper clip to press and release the unit's **RESET** button (shown below).



Soft Reset to Factory Default

If necessary, you can reset the unit to the factory default settings. *This should be done only when you are experiencing problems*. Resetting to the default settings requires you to reconfigure the unit.

To reset to factory default settings:

1. Click **Commands** > **Reset**.
2. Click the **Reset to Factory Default** button. The device configuration parameter values are reset to their factory default values.

If you do not have access to the unit's user interface, you can use the procedure described in Hard Reset to Factory Default as an alternative.

General Configuration Settings

- **System Status:** The Status tab showing the system status is displayed automatically when you log into the Web interface. It is also the default window displayed when you click the **Status** button on the left side of the window. See System Status.
- **System Configuration:** The System Configuration window lets you change the unit's c*ountry*, *system name*, *location name*, and so on (see the window to the right). The Country selection is required to enable the correct radio parameters. The other details help distinguish this unit from other routers, and let you know whom to contact in case of problems. See System Parameters for more information.
- **IP Configuration:** The **IP Configuration** window lets you change the unit's IP parameters. These settings differ between **Routing** and **Bridge** mode. See Network Parameters for more information.
- **Interface Configuration:** The **Interface** configuration pages let you change the Ethernet and Wireless parameters. The **Wireless** tab is displayed by default when you click the **Interfaces** tab.
  - **Ethernet:** To configure the **Ethernet** interface, click **Configure** > **Interfaces** > **Ethernet**. You can set the **Configuration** parameter from this tab for the type of Ethernet transmission. The recommended setting is **auto-speed auto-duplex**. See Ethernet for more information.
  - **Wireless:** To configure the **wireless** interface, click **Configure** > **Interfaces** > **Wireless**. For BSUs, the wireless interface can be placed in either **WORP Base** or **WORP Satellite** mode (selected from the **Interface Type** drop-down box). SUs can be placed only in **WORP Satellite** mode. (See Interface Parameters for more information.)
- **VLAN Configuration:** To configure BSU VLAN parameters, click the **Configure** button followed by the **VLAN** tab; the **BSU Table** tab is displayed. Click the **SUs' Table** tab to configure SU VLAN parameters. Virtual LAN (VLAN) implementation in the Tsunami MP.11 products lets the BSU and SU be used in a VLAN-aware network and processes IEEE 802.1Q VLAN-tagged packets. Network resources behind the BSU and SU can be assigned to logical groups. See VLAN Parameters (BSU Only; Bridge Mode Only) for more information.

Monitoring Settings

The unit offers various facilities to monitor its operation and interfaces. Only the most significant monitoring categories are mentioned here.

- **Wireless:** To monitor the wireless interfaces, click **Monitor** > **Wireless**. This tab lets you monitor the general performance of the radio and the performance of the **WORP Base** or **WORP Satellite** interfaces.
- **Interfaces:** To monitor transmission details, click **Monitor** > **Interfaces**. The **Interfaces** tab provides detailed information about the MAC-layer performance of the wireless network and Ethernet interfaces.
- **Per Station:** Click **Monitor** > **Per Station** to view **Station Statistics**. On the SU, the **Per Station** page shows statistics of the BSU to which the SU is registered. On the BSU, it shows statistics of all the SU's connected to the BSU. The page's statistics refresh every 4 seconds.

Security Settings

To prevent misuse, the 5054 provide wireless data encryption and password-protected access. *Be sure to set the encryption parameters and change the default passwords.*

In addition to Wired Equivalent Privacy (WEP), the units support Advanced Encryption Standard (AES) 128-bit encryption. Two types of the AES encryption are available. Previous releases supported only the AEC-OCB; the AES CCM protocol is now also supported.

Proxim highly recommends you change the **Network Name**, **Encryption Key**, and **Shared Secret** as soon as possible. To do so, click **Configure** > **Interfaces > Wireless**. The encryption key is set using the **Security** tab. For systems that will use roaming features, the **Network Name**, **Encryption Key**, and the **Shared Secret** should each be the same for all SUs that are allowed to roam as well as for all BSUs to which these SUs are allowed to roam.

Encryption

You can protect the wireless data link by using encryption. Encryption keys can be 5 (64-bit), 13 (WEP 128-bit), or 16 (AES 128-bit) characters in length. Both ends of the wireless data link must use the same parameter values. In addition to Wired Equivalent Privacy (WEP), the unit supports Advanced Encryption Standard (AES) 128-bit encryption.

To set the encryption parameters, click **Configure** > **Security** > **Encryption**. See Encryption.

Passwords

Access to the units are protected with passwords. The default password is **public**. For better security it is recommended to change the default passwords to a value (6-32 characters) known only to you.

To change the unit's HTTP, Telnet, or SNMP passwords, click **Configure** > **Management** > **Password**. See Passwords.

Default Settings

Feature	Default
System Name	Tsunami MP.11 5054
Mode of Operation	Bridge
Routing	Disabled
IP Address Assignment Type	Static
IP Address	10.0.0.1
Subnet Mask	255.255.255.0
Default Router IP Address	10.0.0.1
Default TTL	64
RIPv2	Enabled when in Routing Mode
Base Station System Name	Wireless Router
Network Name	OR_WORP
Frequency Channel	Channel 149, Frequency 5.745 GHz (FCC Only devices) DFS Enabled (World Mode devices)
Transmit Power Control	0 dB
Data Rate	36 Mbps
Registration Timeout	5
Network Secret	public
Turbo Mode	Disabled
Channel Bandwidth	20 MHz
Input bandwidth limit (in Kbps)	36032
Output bandwidth limit (in Kbps)	36032
Ethernet Configuration	Auto-Speed Auto-Duplex
Serial port Baud Rate	9600
SNMP Management Interface	Enabled
Telnet Management Interface	Enabled
HTTP Management Interface	Enabled
HTTP Port	80
Telnet Port	23
Telnet Login Timeout	30
Telnet Session Timeout	900
Password	public
Maximum Satellites (per BSU)	250
MAC Authentication	Disabled
Radius Authentication	Disabled
Encryption	Disabled
Static MAC Address Filter	Disabled / No Entries
Ethernet Protocol Filtering	All Filters Disabled
DFS Priority Frequency Channel	Disabled
Announcement Period (when roaming enabled)	100 ms
Multi-Frame Bursting	Enabled
Storm Threshold	Broadcast/Multicast Unlimited

Feature	Default
Broadcast Protocol Filtering	All Protocols Allowed
Dynamic Data Rate Selection	Disabled
Roaming	Disabled
NAT	Disabled
Intra-Cell Blocking	Disabled
Antenna Alignment	Disabled
Country Selection	US-only device – US World device – GB
DHCP Server	Disabled
DHCP Relay	Disabled
Spanning Tree Protocol	Disabled
Antenna Gain (For DFS Threshold compensation)	0
Satellite Density	Large
VLAN Mode	BSU: Transparent Mode SU: Transparent mode when BSU in transparent mode; Trunk mode when BSU in Trunk mode
Access VLAN ID	BSU: N/A; SU: 1
Access VLAN Priority	BSU: N/A; SU: 0
Management VLAN ID	BSU: -1; SU: -1
Management VLAN Priority	BSU: 0; SU: 0
VLAN ID in Trunk VLAN Table	BSU: N/A; SU: 1

Upgrading the Unit

The units are equipped with embedded software that can be updated when new versions are released. Updating the embedded software is described in Web Interface Image File Download. A TFTP server is provided on the product CD; the server is required to transfer the downloaded file to the unit. See TFTP Server Setup.

To access all resolved problems in our solution database, or to search by product, category, keywords, or phrases, go to http://support.proxim.com. You can also find links to drivers, documentation, and downloads at this link.

5 System Status

This chapter describes viewing system status and event log information from the unit's Web Interface.

Click on the **Status** button to access system and event log information. See the following sections:

- Status
- Event Log

Help and Exit buttons also appear on each page of the Web interface; click the **Help** button to access online help; click the **Exit** button to exit the application.

For an introduction to the basics of management, see Basic Management.

Status

The **Status** tab showing the system status is displayed automatically when you log into the Web Interface. It also is the default window displayed when you click the **Status** button on the left side of the window.

The **Status** tab shows the **System Status** and the **System Traps**.

System Status

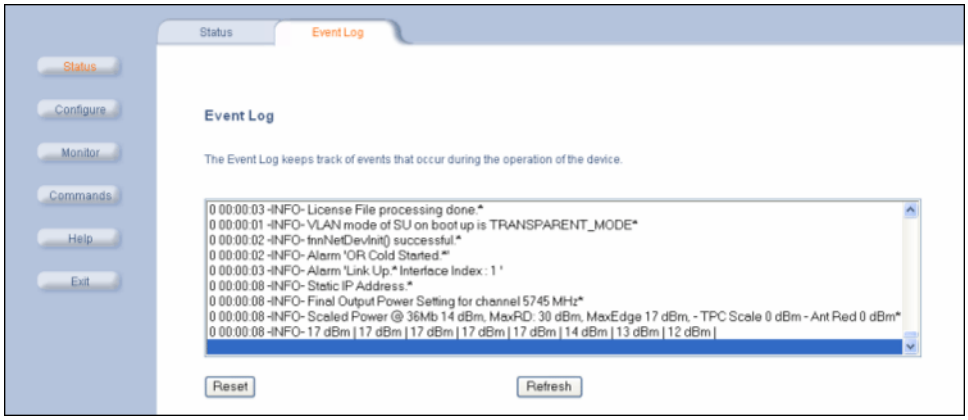
The basic system status is shown in this section, including the version number of the embedded software.

Systems Traps

The status of system traps is shown in this section. System traps occur when the unit encounters irregularities. Deleting system traps has no effect on the operation of the unit. System traps also are sent to an SNMP manager station (if so configured). See "Alarm Traps" in the *Tsunami MP.11/QB.11 Reference Manual* for a list and description of the traps.

Event Log

Click **Status** > **Event Log** to view the contents of your Event Log. The **Event Log** keeps track of events that occur during the operation of the unit. The **Event Log** displays messages that may not be captured by System Traps, such as the **Transmit Power** for the **Frequency Channel** selected.


Status
Event Log
Status
Configure
Monitor
Commands
Help
Exit
Event Log
The Event Log keeps track of events that occur during the operation of the device.
0 00:00:03 -INFO- License File processing done.*
0 00:00:01 -INFO- VLAN mode of SU on boot up is TRANSPARENT_MODE*
0 00:00:02 -INFO- fnnNetDevInit() successful.*
0 00:00:02 -INFO- Alarm 'OR Cold Started.*'
0 00:00:03 -INFO- Alarm 'Link Up.* Interface Index : 1 '
0 00:00:08 -INFO- Static IP Address.*
0 00:00:08 -INFO- Final Output Power Setting for channel 5745 MHz*
0 00:00:08 -INFO- Scaled Power @ 36Mb 14 dBm, MaxRD: 30 dBm, MaxEdge 17 dBm, - TPC Scale 0 dBm - Ant Red 0 dBm*
0 00:00:08 -INFO- 17 dBm | 17 dBm | 17 dBm | 17 dBm | 17 dBm | 14 dBm | 13 dBm | 12 dBm |
Reset
Refresh

See “Event Log Error Messages” in the *Tsunami MP.11/QB.11 Reference Manual* for an explanation of messages that can appear in the Event Log.

6 Configuration

This chapter describes the unit's settings using the unit's Web Interface.

Click the **Configure** button to access configuration settings.

The following topics are discussed in this chapter:

- System Parameters
- Network Parameters
- Interface Parameters
- SNMP Parameters
- Management Parameters
- Security Parameters
- Filtering Parameters
- Intra-Cell Blocking (BSU Only; Bridge Mode Only)
- VLAN Parameters (BSU Only; Bridge Mode Only)
- QoS (Quality of Service) Parameters (BSU Only)
- RIP Parameters (Routing Mode Only)
- NAT (SU Only; Routing Mode Only)

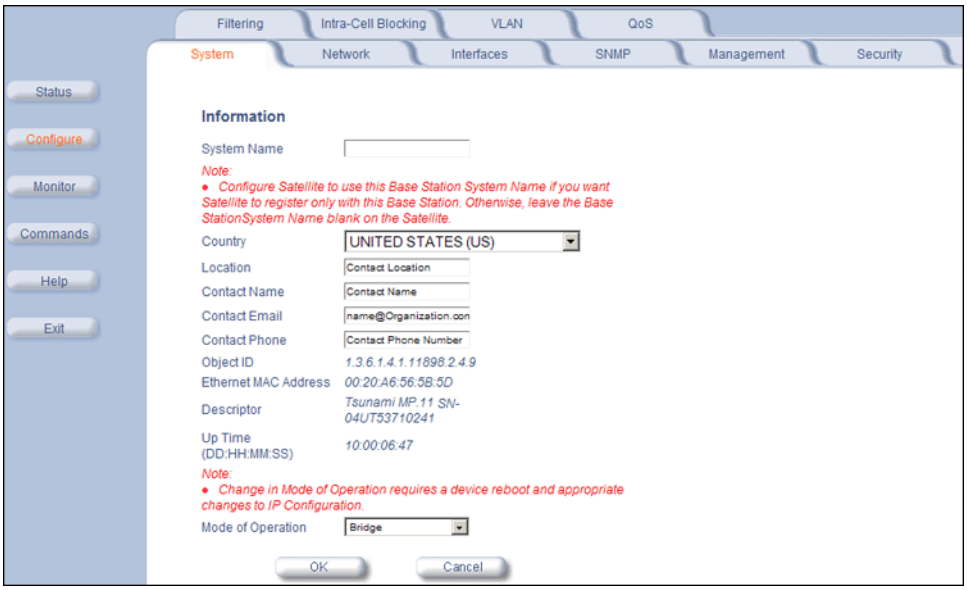
Help and Exit buttons also appear on each page of the Web interface; click the **Help** button to access online help; click the **Exit** button to exit the application.

For an introduction to the basics of management, see Basic Management.

System Parameters

The **System** configuration page lets you change the unit's **System Name**, **Location**, **Mode of Operation**, and so on. These details help you to distinguish the unit from other routers and let you know whom to contact in case you experience problems.

Click **Configure** > **System**; the following window is displayed.



You can view or enter the following details:

- **System Name:** This is the system name for easy identification of the BSU or SU. The System Name field is limited to a length of 32 bytes. Use the system name of a BSU to configure the Base Station System Name parameter on an SU if you want the SU to register only with this BSU. If the Base Station System Name is left blank on the SU, it can register with any Base Station that has a matching Network Name and Network Secret.
- **Country:** Upon choosing a country/band, the Dynamic Frequency Selection (DFS) and Transmit Power Control (TPC) features are enabled automatically if required. The Country selection pre-selects and displays only the allowed frequencies for the selected country/band.

  Click **Configure** > **Interfaces** > **Wireless** to see the channel/frequency list for the selected country/band.

  NOTE: *If **All Channels 5 GHz** is selected from the **Country** drop-down menu, any channel in the 5 GHz range are displayed for manual selection.*

  NOTE: *Units sold only in the United States are pre-configured to scan and display only the outdoor frequencies permitted by the FCC. No other Country selections, channels, or frequencies can be configured. Units sold outside of the United States support the selection of a Country by the professional installer. If you change the Country, a reboot of the unit is necessary for the upgrade to take place.*

  For a non US-only device, the default country selected is **United Kingdom (GB)**.

  Note the following:

  – The channel center frequencies are not regulated; only the band edge frequencies are regulated.
  – If, before upgrade, US was selected as a country for a non US-Only device (which is an incorrect configuration), the country is changed automatically to United Kingdom upon upgrade.

  See Country Codes and Channels for a list of country codes.
- **Location:** This field can be used to describe the location of the unit, for example “Main Lobby.”
- **Contact Name**, **Contact Email**, and **Contact Phone:** In these fields, you can enter the details of the person to contact.
- **ObjectID:** This read-only field shows the OID of the product name in the MIB.
- **Ethernet MAC Address:** This read-only field shows the MAC address of the Ethernet interface of the device.
- **Descriptor:** This read-only field shows the product name and firmware build version.
- **Up Time:** This read-only field shows the length of time the device has been up and running since the last reboot.

- **Mode of Operation:** This drop-down menu is used to set the unit as a **bridge** (layer 2) or as a **router** (layer 3). See Bridge and Routing Modes for more information.

Bridge and Routing Modes

Bridge Mode

A bridge is a product that connects a local area network (LAN) to another LAN that uses the same protocol (for example, Ethernet). You can envision a bridge as being a device that decides whether a message from you to someone else is going to the LAN in your building or to someone on the LAN in the building across the street. A bridge examines each message on a LAN, passing those known to be within the same LAN, and forwarding those known to be on the other interconnected LAN (or LANs).

In bridging networks, computer or node addresses have no specific relationship to location. For this reason, messages are sent out to every address on the network and are accepted only by the intended destination node. Bridges learn which addresses are on which network and develop a learning table so that subsequent messages can be forwarded to the correct network.

Bridging networks are generally always interconnected LANs since broadcasting every message to all possible destination would flood a larger network with unnecessary traffic. For this reason, router networks such as the Internet use a scheme that assigns addresses to nodes so that a message or packet can be forwarded only in one general direction rather than forwarded in all directions.

A bridge works at the data-link (physical) layer of a network, copying a data packet from one network to the next network along the communications path.

The default Bridging Mode is **Transparent Bridging**.

This mode works if you do not use source routing in your network. If your network is configured to use source routing, then you should use either Multi-Ring SRTB or Single-Ring SRTB mode.

In Multi-Ring SRTB mode, each unit must be configured with the Bridge number, Radio Ring number, and Token Ring number. The Radio Ring number is unique for each Token Ring Access Point and the Bridge number is unique for each Token Ring Access Point on the same Token Ring segment.

Alternatively, you may use the Single-Ring SRTB mode. In this mode, only the Token Ring number is required for configuration.

Routing Mode

Routing mode can be used by customers seeking to segment their outdoor wireless network using routers instead of keeping a transparent or bridged network. By default the unit is configured as a bridge device, which means traffic between different outdoor locations can be seen from any point on the network.

By switching to routing mode, your network now is segmented by a layer 3 (IP) device. By using Routing mode, each network behind the BSU and SUs can be considered a separate network with access to each controlled through routing tables.

The use of a router on your network also blocks the retransmission of broadcast and multicast packets on your networks, which can help to improve the performance on your outdoor network in larger installations.

The use of Routing mode requires more attention to the configuration of the unit and thorough planning of the network topology of your outdoor network. The unit can use Routing mode in any combination of BSU and SUs. For example, you may have the BSU in Routing mode and the SU in Bridge mode, or vice versa.

When using Routing mode, pay close attention to the configuration of the default gateway both on your unit and on your PCs and servers. The default gateway controls where packets with unknown destinations (Internet) should be sent. Be sure that each device is configured with the correct default gateway for the next hop router. Usually this is the next router

on the way to your connection to the Internet. You can configure routes to other networks on your Intranet through the addition of static routes in your router's routing table.

Key Reasons to Use Routing Mode

One key reason why customers would use Routing mode is to implement virtual private networks (VPNs) or to let nodes behind two different SUs communicate with each other. Many customers do this same thing in Bridging mode by using secondary interfaces on the router at the BSU or virtual interfaces at the BSU in VLAN mode to avoid some of the drawbacks of IP Routing mode.

Routing mode prevents the transport of non-IP protocols, which may be desirable for Service Providers.

Routing mode is usually more efficient because Ethernet headers are not transported and non-IP traffic is blocked.

Benefits of using Routing Mode

- Enabling RIP makes the unit easier to manage for a Service Provider that uses RIP to dynamically manage routes. RIP is no longer very common for Service Providers or Enterprise customers and an implementation of a more popular routing protocol like OSPF would be desirable.
- Routing mode saves bandwidth by not transporting non-IP protocols users might have enabled, like NetBEUI or IPX/SPX, which eliminates the transmission of broadcasts and multicasts.
- The MAC header is:
    - Destination MAC: 6 bytes
    - Source MAC: 6 bytes
    - Ethernet Type: 2 bytes

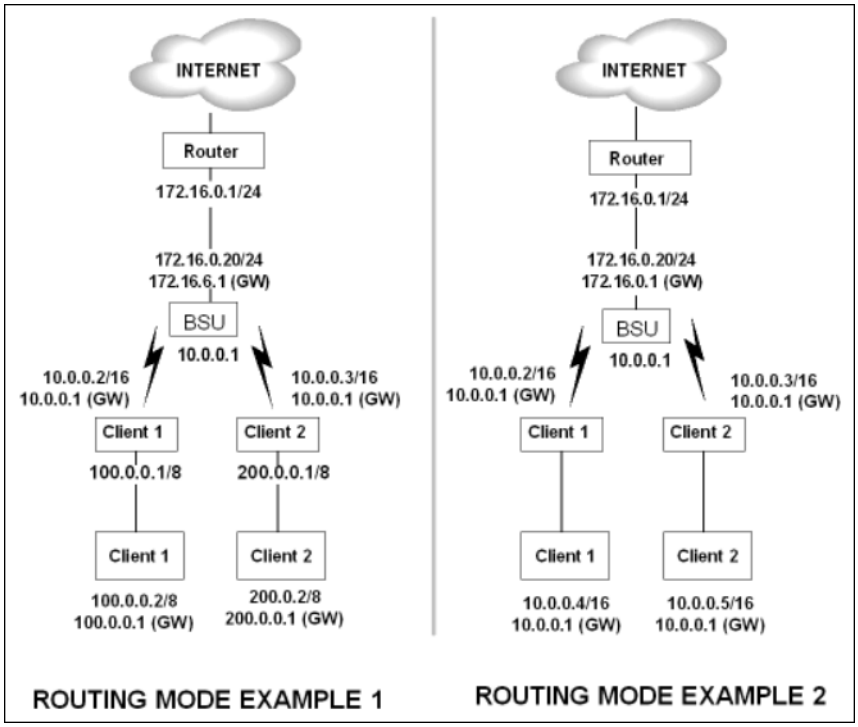
If the average packet size is 1000 bytes, the overhead saved is 1.5%; with a frame size of 64 bytes, the overhead saved is 20%; and for frame sizes of 128 bytes, the saving is 10%. Network researchers claim that most network traffic consists of frames smaller than 100 bytes.

In order to support routers behind the SUs with multiple subnets and prevent routing loops, you want individual routes (and more than one) per SU.

Routing Mode Examples

In the first example, both the BSU and the SUs are configured for Routing mode. This example is appropriate for businesses connecting remote offices that have different networks.

In example 2, the BSU is in Routing mode and the SUs are in Bridge mode. Notice the PCs behind the SUs must configure their default gateways to point to the BSU, not the SU.



Notes:

- One of the most important details to pay attention to in Routing mode are the unit's and the PC's default gateways. It is a common mistake to set up the PC's gateway to point to the SU when the SU is in Bridge mode and the BSU is in Routing mode. Always check to make sure the PCs on your network are configured to send their IP traffic to the correct default gateway.
- Be sure to reboot the unit to permanently save static routes. New routes take effect immediately without a reboot, but are not permanently saved with your configuration until you do reboot the device. An unexpected power outage could cause static routes you entered to "disappear" when the unit reboots if they have not been saved. You also should save a copy of your unit's configuration file in case the unit must be reloaded. This saves you from being required to re-enter numerous static routes in a large network.
- The routing table supports up to 500 static routes.

Network Parameters

The Network tab contains the following sub-tabs. Note that the availability of some sub-tabs depends on whether the unit is in Bridge or Routing Mode.

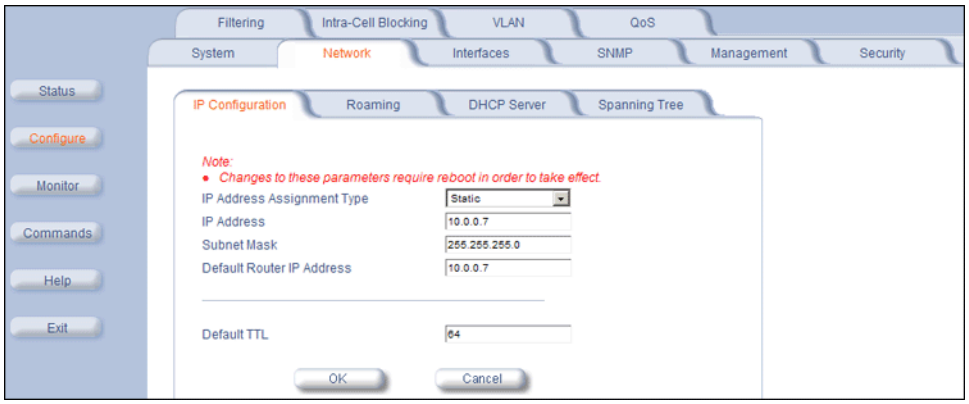
- IP Configuration
- Roaming
- DHCP Server
- Spanning Tree (Bridge Mode Only)
- IP Routes (Routing Mode Only)
- DHCP Relay Agent (Routing Mode Only)

IP Configuration

Click **Configure** > **Network** > **IP Configuration** to view and configure local IP address information. Configurable settings differ between **Bridge** mode and **Routing** mode.

Bridge Mode

If the device is configured in **Bridge** mode, the following screen is displayed:



Configure or view the following parameters:

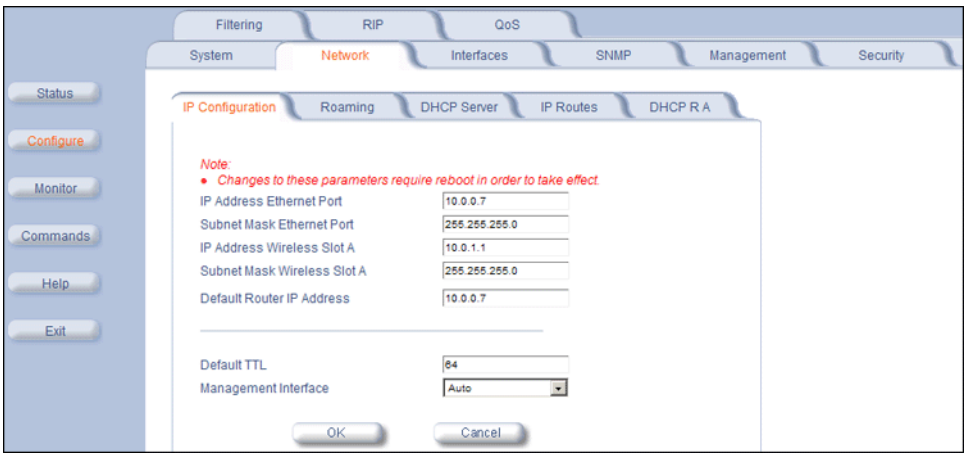
- **IP Address Assignment Type**:
  - Select ***Static*** if you want to assign a static IP address to the unit. Use this setting if you do not have a DHCP server or if you want to manually configure the IP settings
  - Select ***Dynamic*** to have the device run in DHCP client mode, which gets an IP address automatically from a DHCP server over the network.

When the unit is in **Bridge** mode, only one IP address is required. This IP address also can be changed with ScanTool (see Setting the IP Address with ScanTool). In **Routing** mode, both Ethernet and Wireless interfaces require an IP address.

- **IP Address:** The unit's static IP address (default IP address is 10.0.0.1). This parameter is configurable only if the IP Address Assignment Type is set to **Static**.
- **Subnet Mask:** The mask of the subnet to which the unit is connected (the default subnet mask is 255.255.255.0). This parameter is configurable only if the IP Address Assignment Type is set to **Static**.
- **Default Router IP Address:** The IP address of the default gateway. This parameter is configurable only if the IP Address Assignment Type is set to **Static**.
- **Default TTL:** The default time-to-live value.

Routing Mode

If the device is configured in **Routing** mode, both Ethernet and Wireless interfaces require an IP address. The following screen is displayed:



Configure or view the following parameters:

- **IP Address Ethernet Port:** The unit's Ethernet IP address. The default is 10.0.0.1.
- **Subnet Mask Ethernet Port:** The unit's Ethernet IP address subnet mask.The default is 255.255.255.0.
- **IP Address Wireless Slot A:** The unit's wireless IP address. The default is 10.0.0.1.
- **Subnet Mask Wireless Slot A:** The unit's wireless IP address subnet mask.
- **Default Router IP Address:** The router's IP address.
- **Default TTL:** The default time-to-live value.
- **Management Interface:** The interface used to manage the device. Select Ethernet, Wireless, or Auto.

Roaming

Roaming Overview

Roaming is a feature by which an SU terminates the session with the current BSU and starts the registration procedure with another BSU when it finds the quality of the other BSU to be better. Roaming provides MAC level connectivity to the SU that roams from one BSU to another. Roaming takes place across the range of frequencies that are available per configuration. The current release offers handoff times of up to a maximum of 80 ms. This is fast enough to allow the SU to seamlessly roam from one BSU to the other therefore supporting session persistence for delay-sensitive applications. The feature also functions as BSU backup in case the current BSU fails or becomes unavailable.

The Roaming feature lets the SU monitor local SNR and data rate for all frames received from the current BSU. As long as the average local SNR for the current BSU is greater than the slow scanning threshold, and the number of retransmitted frames is greater than the slow scanning threshold given in percentage, the SU does not scan other channels for a better BSU.

- The ***normal scanning*** procedure starts when the average local SNR for the current BSU is less than or equal to the slow scanning threshold and the number of retransmitted frames is greater than the slow scanning threshold given in percentage. During the normal scanning procedure the SU scans the whole list of active channels while maintaining the current session uninterrupted.
- ***Fast scanning*** is the scanning procedure performed when the average local SNR for the current BSU is very low (below the fast scanning threshold) and the number of retransmitted frames is greater than the fast scanning retransmission threshold given in%, so that the current session should terminate as soon as possible. During this procedure, the SU scans other active channels as fast as possible.

Roaming can only occur if the normal scanning or fast scanning procedure is started under the following conditions:

1. If the roaming is started from the normal scanning procedure (after the SU scans all the active channels), the SU selects the BSU with the best SNR value on all available channels. The SU roams to the best BSU only if the SNR value for the current BSU is still below the slow scanning SNR threshold, and best BSU offers a better SNR value for at least roaming threshold than the current BSU. The SU starts a new registration procedure with the best BSU without ending the current session.
2. If the roaming is started from the fast scanning procedure, the SU selects the first BSU that offers better SNR than the current BSU, and starts a new registration procedure with the better BSU without ending the current session.

Roaming with Dynamic Data Rate Selection (DDRS) Enabled

When an SU roams from BSU-1 to BSU-2 and DDRS is enabled, the data rate at which the SU connects to BSU-2 is the default DDRS data rate. If this remains at the factory default of 6 Mbps, there can be issues with the application if it requires more than 6 Mbps (for example, multiple video streams).

Applications requiring a higher data rate could experience a slight data loss during the roaming process while DDRS selects a higher rate (based upon link conditions).

When the applications re-transmit at a possibly slower rate, the WORP protocol initially services the data at 6 Mbps and increases the data rate up to the "Maximum DDRS Data Rate" (*ddrsmaxdatarate*) one step at a time. Because the applications are not being serviced at the best possible rate, they further slow down the rate of data send.

The DDRS algorithm requires data traffic (a minimum of 128 frames) to raise the rate to a higher value. Although roaming occurs successfully, the previous scenario causes applications to drop their sessions; hence session persistence is not maintained.

For more information on DDRS, see Dynamic Data Rate Selection (DDRS).

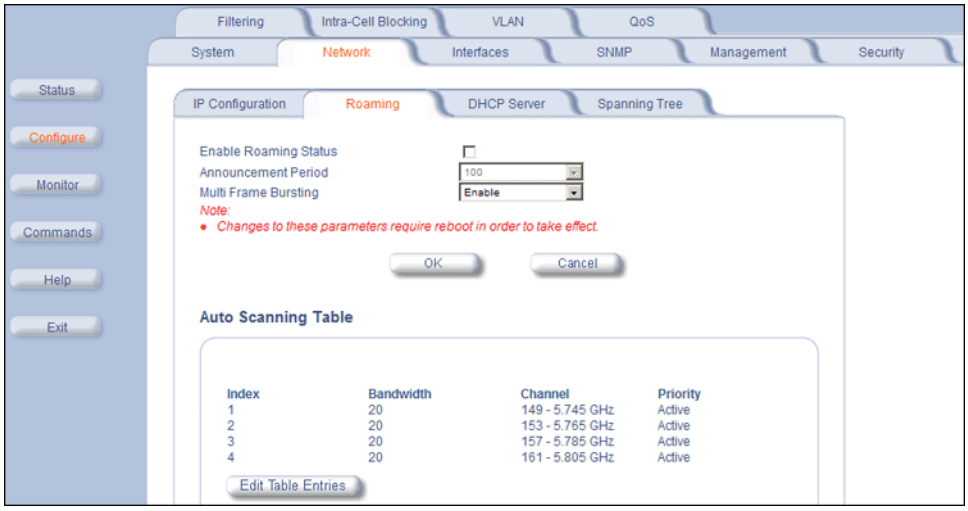
NOTE: *You must know the data rate required for the applications running and you must ensure (during network deployment) that the ranges and RF links can support the necessary data rate. You also must set the default DDRS data rate at the capacity necessary for the application so that it connects to the next Base Station at the required capacity if roaming occurs. Set the "Default DDRS Data Rate" (ddrsdefdatarate) to a greater value (24, 36, 48 or 54 Mbps, for example) for applications requiring session persistence when roaming occurs.*

Roaming Configuration

Click **Configure** > **Network** > **Roaming** to configure Roaming.

The screen differs depending on whether the unit is configured as a BSU or as an SU.

BSU Roaming Configuration



View or set the following parameters:

- **Enable Roaming Status**: Enable or disable the Roaming feature by selecting or de-selecting the checkbox. The default value is disabled (clear).
- **Announcement Period**: If you enable roaming, you may set the Announcement Period for a value between 25 to 100 ms. The default is 100 ms.
- **Multi-Frame Bursting**: The default value is enabled.
- **Auto Scanning Table**: See description below.

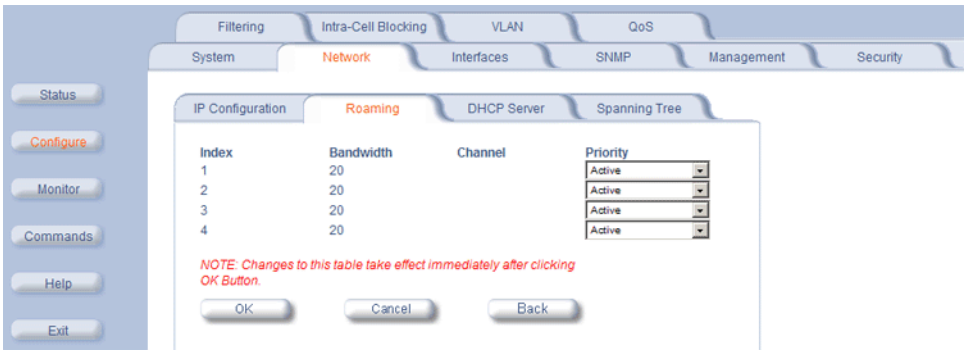
Auto Scanning Table

An SU scans all available channels for a given bandwidth during roaming. In order to reduce the number of channels an SU has to scan and thus decrease the roaming time, a channel priority list that tells the SU what channels to scan is implemented. Each channel in the channel priority list is specified with its corresponding bandwidth and the priority with which it should be scanned, either “Active” (standard priority), “Active High” (high priority), or “Inactive”.

An SU will scan all channels indicated as “Active” during roaming. However, it will scan active channels indicated as “High Priority” before scanning active channels indicated as standard priority. Channels that are not going to be used in the wireless network should be configured as “Inactive” so that the SU can skip over those channels during scanning saving this way time.

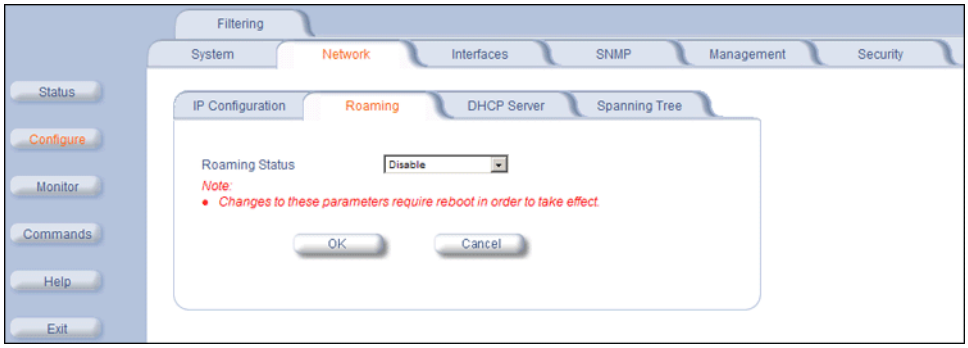
A BSU broadcasts the channel priority list to all valid authenticated SUs in its sector. It re-broadcasts the channel priority list to all SUs every time the list is updated on the BSU.

Click **Edit Table Entries** to make changes; enter your changes and click **OK**.



SU Roaming Configuration

Enable or disable the Roaming feature in the **Roaming Status** drop-down box. The default value is disabled.



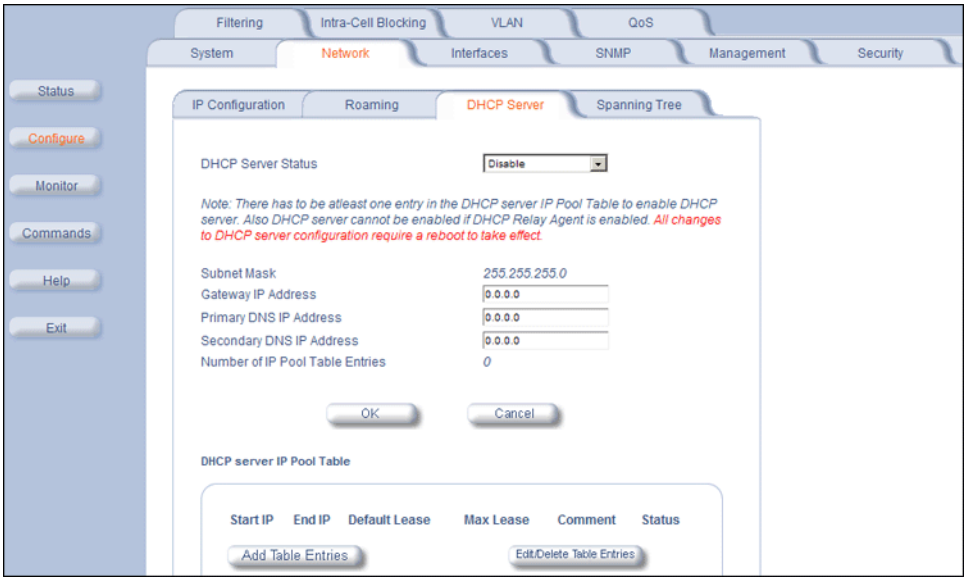
NOTE: *To enable roaming, you must enable* **Roaming Status** *on both the BSU and the SU.*

DHCP Server

When enabled, the DHCP server allows allocation of IP addresses to hosts on the Ethernet side of the SU or BSU. Specifically, the DHCP Server feature lets the SU or BSU respond to DHCP requests from Ethernet hosts with the following information:

- Host IP address
- Gateway IP address
- Subnet Mask
- DNS Primary Server IP address
- DNS Secondary Server IP

Click **Configure** > **Network** > **DHCP Server** to enable the unit on a DHCP Server.



The following parameters are configurable:

- **DHCP Server Status:** Verify that DHCP Relay Agent is disabled. After you have made at least one entry in the DHCP server IP Pool Table, enable DHCP Server by selecting **Enable** from the **DHCP Server Status** pull-down menu.

NOTE: *There must be at least one entry in the DHCP server IP Pool Table to enable DHCP server. Also, DHCP server cannot be enabled if DHCP Relay Agent is enabled.*

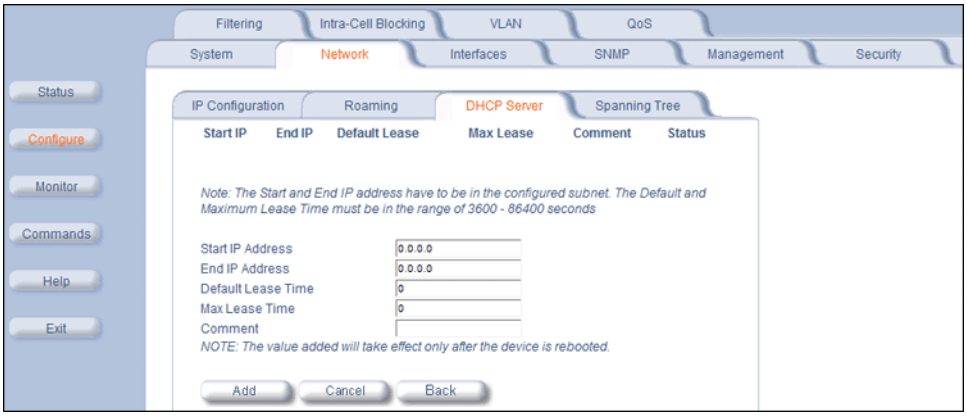
- **Subnet Mask:** The unit supplies this subnet mask in its DHCP response to a DHCP request from an Ethernet host. Indicates the IP subnet mask assigned to hosts on the Ethernet side using DHCP.
- **Gateway IP Address:** The unit supplies this gateway IP address in the DHCP response. It indicates the IP address of a router assigned as the default gateway for hosts on the Ethernet side. This parameter must be set.
- **Primary DNS IP Address:** The unit supplies this primary DNS IP address in the DHCP response. It indicates the IP address of the primary DNS server that hosts on the Ethernet side uses to resolve Internet host names to IP addresses. This parameter must be set.
- **Secondary DNS IP Address:** The unit supplies this secondary DNS IP address in the DHCP response.
- **Number of IP Pool Table Entries:** The number of IP pool table entries is a read-only field that indicates the total number of entries in the DHCP server IP Pool Table. See Add Entries to the DHCP Server IP Pool Table.

Add Entries to the DHCP Server IP Pool Table

You can add up to 20 entries in the IP Pool Table. An IP address can be added if the entry's network ID is the same as the network ID of the device.

NOTE: *After adding entries, you must reboot the unit before the values take effect.*

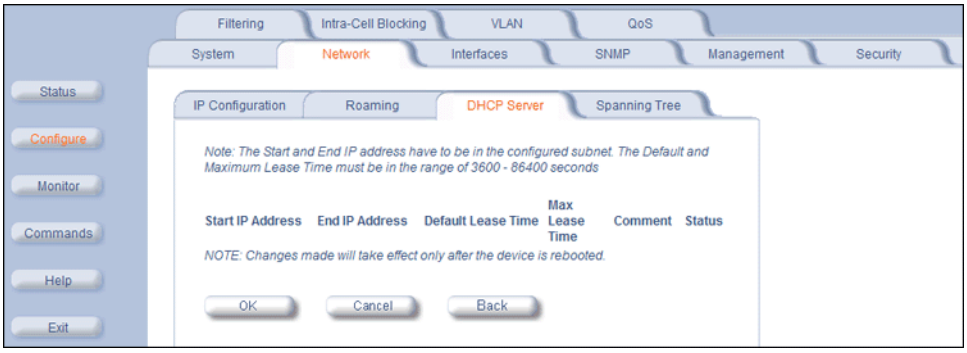
1. To add an entry click **Add Table Entries**.



2. Enter the following parameters and click **Add**:
   - **Start IP Address:** Indicates the starting IP address that is used for assigning address to hosts on the Ethernet side in the configured subnet.
   - **End IP Address:** Indicates the ending IP address that is used for assigning address to hosts on the Ethernet side in the configured subnet.
   - **Default Lease Time:** Specifies the default lease time for IP addresses in the address pool. The value is 3600-86400 seconds.
   - **Max Lease Time:** The maximum lease time for IP addresses in the address pool. The value is 3600-86400 seconds.
   - **Comment:** The comment field is a descriptive field of up to 255 characters.

Edit/Delete Entries in the DHCP Server IP Pool Table

1. Click **Edit/Delete Table Entries** to make changes
2. Enter your changes and click **OK**.



Spanning Tree (Bridge Mode Only)

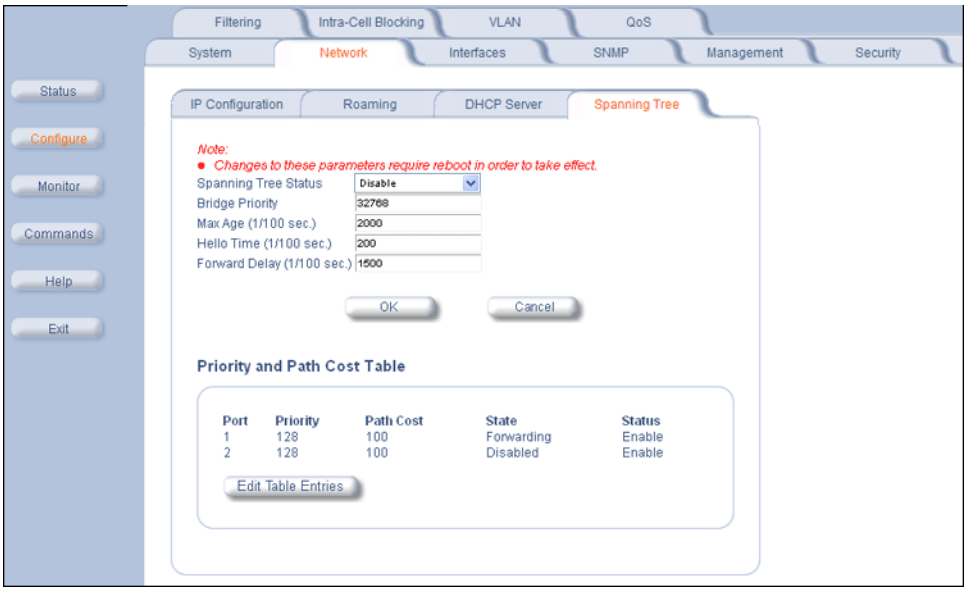
NOTE: *The unit must be in Bridge mode to configure Spanning Tree.*

This protocol is executed between the bridges to detect and logically remove redundant paths from the network. Spanning Tree can be used to prevent link-layer loops (broadcast is forwarded to all port where another device may forward it and, finally, it gets back to this unit; therefore, it is looping). Spanning Tree can also be used to create redundant links and operates by disabling links: hot standby customer is creating a redundant link without routing function.

If your network does not support Spanning Tree, be careful to avoid creating network loops between radios. For example, creating a WDS link between two units connected to the same Ethernet network creates a network loop (if spanning tree is disabled).

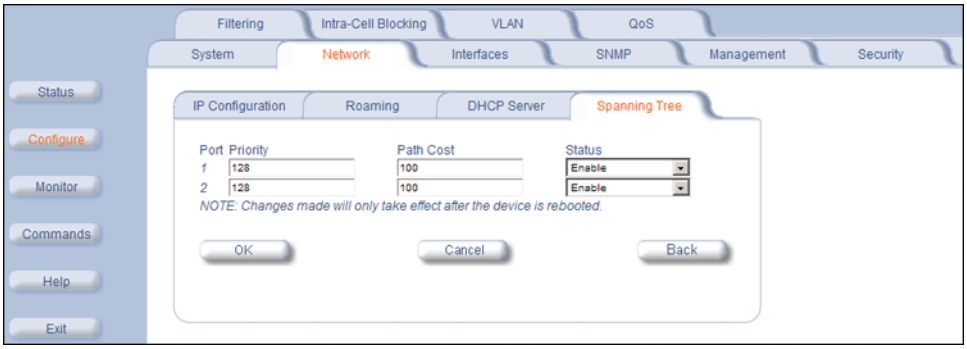
The Spanning Tree configuration options are advanced settings. Proxim recommends that you leave these parameters at their default values unless you are familiar with the Spanning Tree protocol.

Click the **Spanning Tree** tab to change Spanning Tree values.



Edit/Disable Entries in the Priority and Path Cost Table

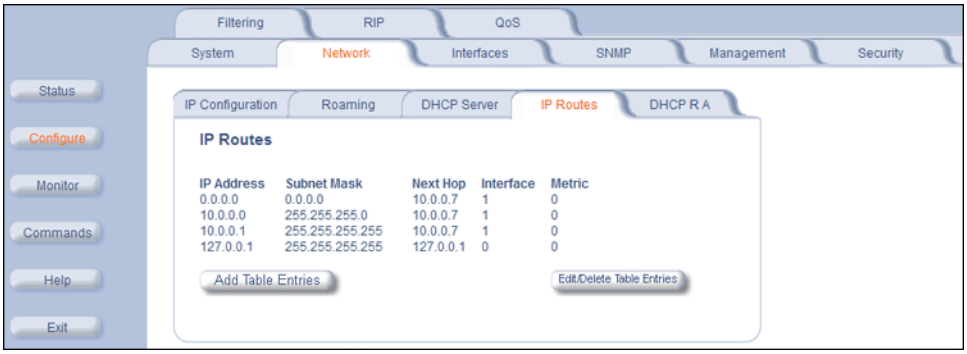
1. Click **Edit Table Entries** to make changes
2. Enter your changes and click **OK**.



IP Routes (Routing Mode Only)

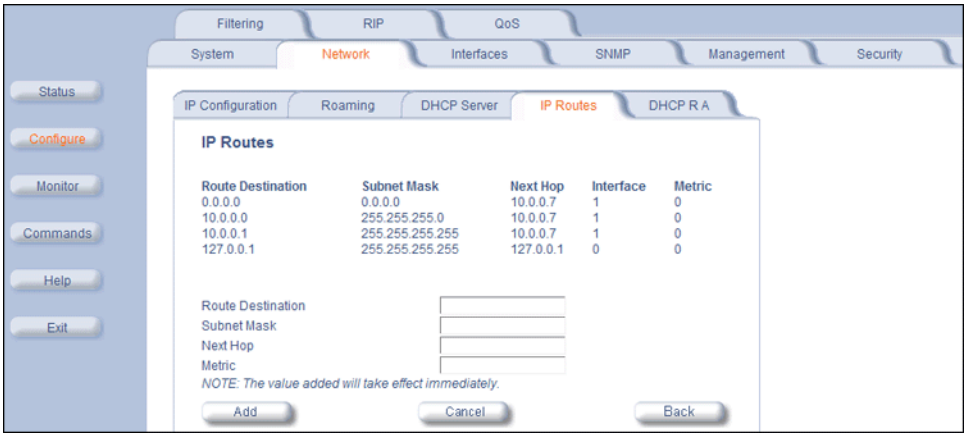
NOTE: *The unit must be in Routing mode to configure IP Routes.*

Click **Configure** > **Network** > **IP Routes** to configure.



Add IP Routes

1. Click the **Add** button; the following screen is displayed.

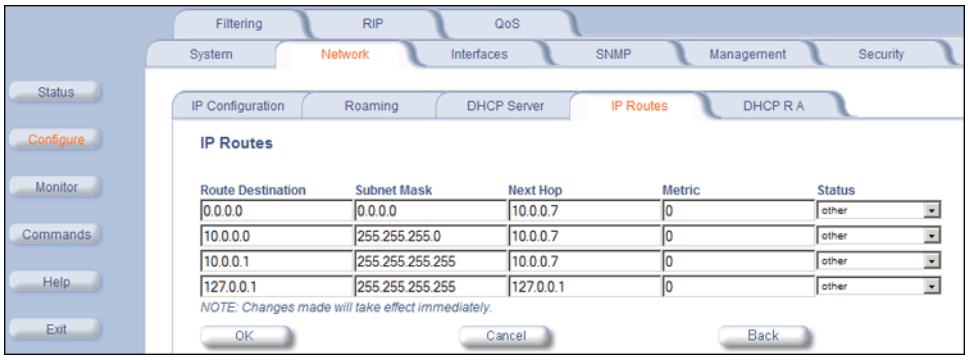


2. Enter the route information.
3. Click **Add**. The **IP Address** and **Subnet Mask** combination is validated for a proper combination.

NOTE: *When adding a new entry, the IP address of the Route Destination must be in either the Ethernet subnet or in the wireless subnet of the unit.*

Edit/Delete IP Routes

1. Click the **Edit/Delete Table Entries** button.



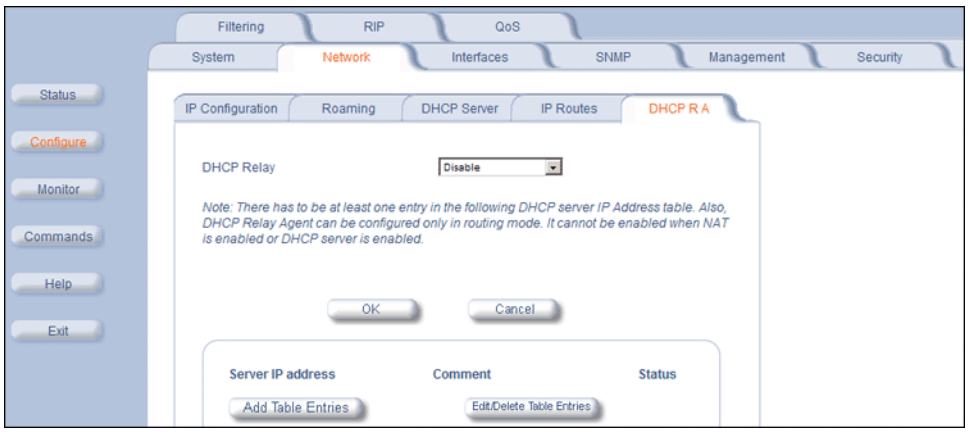
2. Edit the route information.
3. Click **OK**. The IP address and subnet mask combination is validated for a proper combination.

DHCP Relay Agent (Routing Mode Only)

NOTE: *The unit must be in Routing mode to configure DHCP Relay Agent.*

Click **Configure** > **Network** > **DHCP RA** to enable the unit's DHCP Relay Agent. When enabled, the DHCP relay agent forwards DHCP requests to the set DHCP server. There must be at least one entry in the corresponding Server IP Address table in order to enable the DHCP Relay Agent.

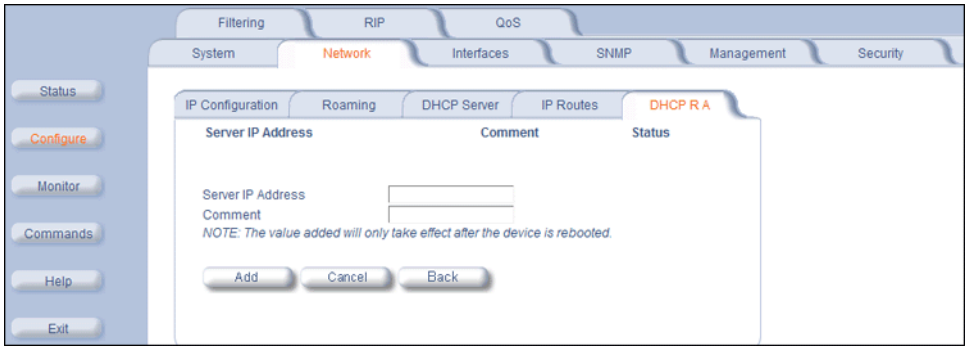
Note that DHCP Relay Agent parameters are configurable only in **Routing** mode. It cannot be enabled when NAT or DHCP Server is enabled.



Add Entries to the DHCP Relay Agent Table

To add entries to the table of DHCP Relay Agents:

1. Click **Add Table Entries**; the following window is displayed:

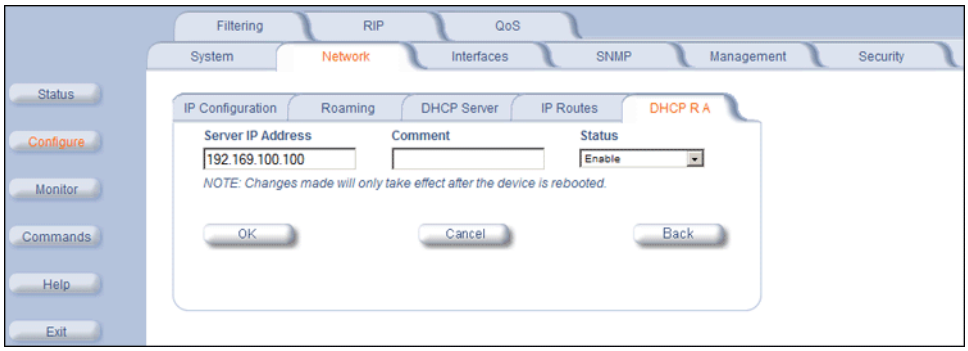


2. Enter the **Server IP Address** and any optional comments, and click **Add**.

Edit/Delete Entries in the DHCP Relay Agent Table

To edit or delete entries in the table of DHCP Relay Agents:

1. Click **Edit/Delete Table Entries**. The following window is displayed:



2. Enter your changes, and click **OK**.

Interface Parameters

The Interface tab contains the following sub-tabs.

- Wireless
  - Base Mode
  - Satellite Mode
- Ethernet

Wireless

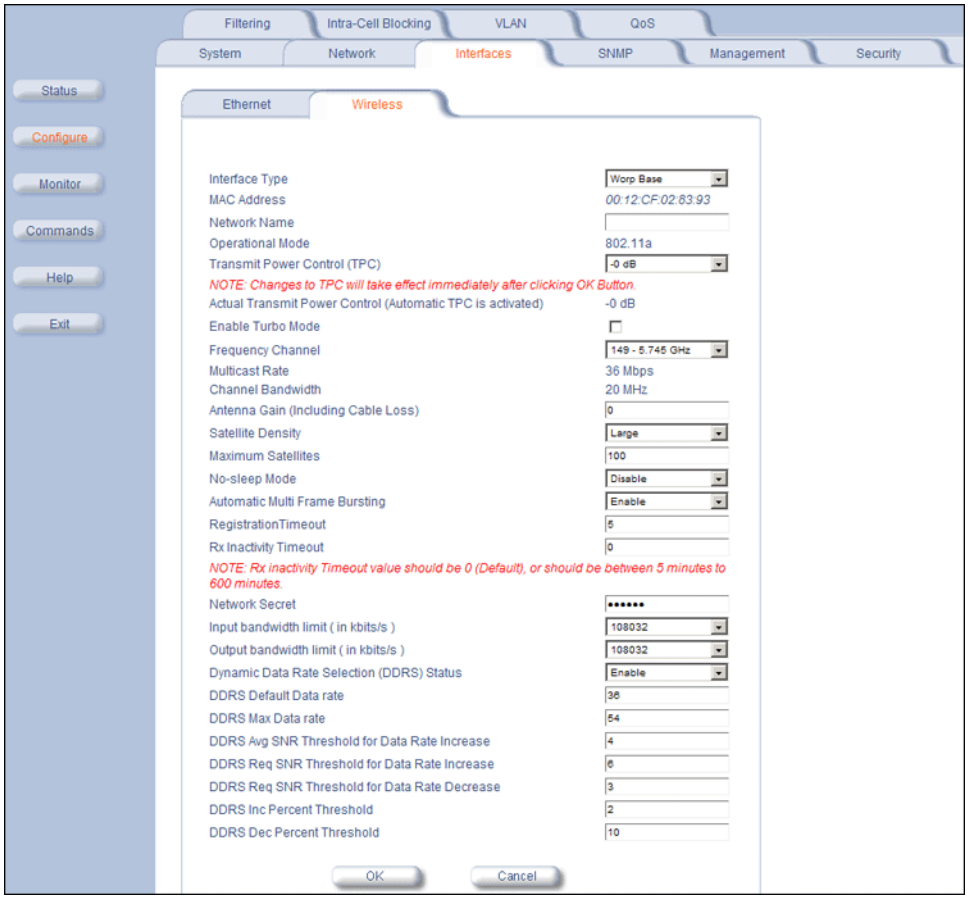
To configure the wireless interface, click **Configure** > **Interfaces** > **Wireless**.

For Base Station units, the wireless interface can be placed in either WORP Base or WORP Satellite mode (selected from the **Interface Type** drop-down box). SUs can be placed only in WORP Satellite mode. The wireless interface settings depend upon whether the mode is Base or Satellite.

The Wireless Outdoor Router Protocol (WORP) is a polling algorithm designed for wireless outdoor networks. WORP takes care of the performance degradation incurred by the so-called “hidden-node” problem, which can occur when wireless LAN technology is used for outdoor building-to-building connectivity. In this situation, when multiple radios send an RTS, if another radio is transmitting, it corrupts all data being sent, degrading overall performance. The WORP polling algorithm ensures that these collisions cannot occur, which increases the performance of the overall network significantly.

WORP dynamically adapts to the number of SUs that are active on the network and the amount of data they have queued to send.

Base Mode



The following parameters may be configured or viewed:

- **Interface Type:** The interface type can be **WORP Satellite** or **WORP Base**.
- **MAC Address:** The factory-assigned MAC address of the unit. This is a read-only field.
- **Network Name:** A Network Name is a name given to a network so that multiple networks can reuse the same frequency without problems. An SU can only register to its base if it has the same Network Name. The Network Name is one of the parameters that allow a Subscriber Unit to register on a Base Station. The **Base Station System Name** and **Frequency Channel** also are parameters to guide the SU to the proper BSU on the network, but they provide no security. Basic security is provided through encryption, as it causes none of the messages to be sent in the clear. Further security is provided by mutual authentication of the BSU and SU using the **Network Secret**. The Network Name can be 2 to 32 characters in length.
- **Operational Mode:** This field indicates the operational mode of the unit depending upon the specific Tsunami MP.11. This operational mode cannot be changed as it is based upon a license file.
- **Transmit Power Control (TPC):** By default, the unit lets you transmit at the maximum output power for the country/band or regulatory domain and frequency selected. However, with Transmit Power Control (TPC), you can adjust the output power of the unit to a lower level in order to reduce interference to neighboring devices or to use a higher gain antenna without violating the maximum radiated output power allowed for your country/band. Also, some countries/bands that require DFS also require the transmit power to be set to a 6 dB lower value than the maximum allowed EIRP when link quality permits. You can see your unit's current output power for the selected frequency in the event log.

  The event log shows the selected power for all data rates, so you must look up the proper data rate to determine the actual power level.

NOTE: *This feature only lets you decrease your output power; it does not let you increase your output power beyond the maximum allowed defaults for your frequency and country.*

Select one of the following options and click **OK** at the bottom of the window. Your original output power is adjusted relative to the value selected. The new setting takes effect immediately without rebooting:

TPC Selection (dB)	Maximum TX Power (dBm)
0 (default)	16
-3	13
-6	10
-9	7
-12	4
-15	1
-18 (minimum TPC level)	0

NOTE: *24 Mbps and lower modulation have maximum +16 dBm TX power, 36 Mbps has maximum +13 dBm TX power, 48 Mbps has maximum +12 dBm TX power, and 54 Mbps has maximum +11 dBm TX power. Because higher modulation has a lower maximum TX power, the total TPC range is smaller at a higher data rate. Because the minimum TX power is equal for all data rates, each TPC selection has constant TX power for all data rates except where the maximum TX power is limited.*

- **Actual Transmit Power Control:** This field displays the actual transmit power when ATPC is enabled.
- **Enable Turbo Mode *(Non-DFS US Only)*:** Check this box to enable Turbo Mode. **Turbo Mode is supported only in the United States when DFS is not required.** Enabling turbo mode, in its current implementation, allows the unit to use two adjacent frequency channels to transmit and receive a signal. By enabling turbo mode, the receive sensitivity improves by 4 dB for the 36 Mbps data rate and by 2 dB for the 24 Mbps data rate.

  NOTE: *The additional sensitivity is provided with the impact of using twice as much spectrum and thus increasing the opportunity of interference and decreased ability for system collocation. Generally, Turbo mode is not recommended except when the extra sensitivity is absolutely required.*

- **Frequency Channel:** The frequency channel indicates the band center frequency the unit uses for communicating with peers. This frequency channel can be set in several ranges, depending upon regulatory domain. Refer to Country Codes and Channels for channelization information. For countries in which DFS is not required, the **Frequency Channel** list displays only the channels and frequencies allowed for the selected country/band.

  In countries and bands in which DFS is required, **Frequency Channel** is not configurable. Instead the channel is auto-selected by the DFS process.
- **Multicast Rate:** The rate at which data is to be transferred. This drop down box is unavailable when DDRS is enabled.

  The default multicast rate for the unit is 36 Mbps. The SU must never be set to a lower data rate than the BSU, because timeouts will occur at the BSU and communication will fail.

  Selections for multicast rate are shown in the following table:

Multicast Rates in Mbps	Multicast Rates in Mbps with Turbo Mode Enabled (Non-DFS US Only)
6	12
9	18
12	24
18	36
24	48
36	72
48 (see note)	96 (see note)

Multicast Rates in Mbps	Multicast Rates in Mbps with Turbo Mode Enabled (Non-DFS US Only)
54 (see note)	108 (see note)

NOTE: *If you select 48 or 54 Mbps (96 or 108 in Turbo mode) DDRS is automatically turned on.*

- **Channel Bandwidth:** This is a read only field. Channel Bandwidth is set at 20 MHz.
- **Antenna Gain** You can modify the sensitivity of the radio card when detecting radar signals in accordance with ETSI, FCC, and IC Dynamic Frequency Selection (DFS) requirements. Given the radar detection threshold is fixed by ETSI, the FCC, and IC and that a variety of antennas with different gains may be attached to the unit, you must adjust this threshold to account for higher than expected antenna gains and avoid false radar detection events. This can result in the units constantly changing frequency channels.

  You can configure the threshold for radar detection at the radio card to compensate for increased external antenna gains.

  The Antenna Gain value ranges from 0 to 35. The default value is 0.
- **Satellite Density:** The **Satellite Density** setting is a valuable feature for achieving maximum bandwidth in a wireless network. It influences the receive sensitivity of the radio interface and improves operation in environments with a high noise level. Reducing the sensitivity of the unit enables unwanted “noise” to be filtered out (it disappears under the threshold).

  You can configure the **Satellite Density** to be **Large**, **Medium**, **Small**, **Mini**, or **Micro**. The default value for this setting is Large. The smaller settings are appropriate for high noise environments; a setting of **Large** would be for a low noise environment.

  A long distance link may have difficulty maintaining a connection with a small density setting because the wanted signal can disappear under the threshold. Consider both noise level and distance between the peers in a link when configuring this setting. The threshold should be chosen higher than the noise level, but sufficiently below the signal level. A safe value is 10 dB below the present signal strength.

  If the Signal-to-Noise Ratio (SNR) is not sufficient, you may need to set a lower data rate or use antennas with higher gain to increase the margin between wanted and unwanted signals. In a point-to-multipoint configuration, the BSU should have a density setting suitable for all of its registered SUs, especially the ones with the lowest signal levels (longest links).

  Take care when configuring a remote interface; check the available signal level first, using Remote Link Test.

  WARNING: When the remote interface accidentally is set at too small a value and communication is lost, it cannot be reconfigured remotely and a local action is required to bring the communication back. Therefore, the best place to experiment with the level is at the unit that can be managed without going through the link; if the link is lost, the setting can be adjusted to the correct level to bring the link back.

  Sensitivity threshold settings related to the density settings for the unit are:

Satellite Density	Receive Sensitivity Threshold	Defer Threshold
Large	-95 dBm	-62 dBm
Medium	-86 dBm	-62 dBm
Small	-78 dBm	-52 dBm
Mini	-70 dBm	-42 dBm
Micro	-62 dBm	-36 dBm

- **Maximum Satellites:** You can specify a maximum value of 250 in this field, because up to 250 SUs can be connected to a BSU. If a BSU already has as many SUs as specified in this field, a new SU cannot connect to the BSU.

- **No-Sleep Mode:** No-Sleep Mode was a feature used to control jitter in Tsunami MP.11 products running 2.2.6, and earlier, versions of software. The introduction of QoS and the new WORP resource scheduling mechanism have eliminated the need for No-Sleep Mode. Furthermore, QoS provides better control over jitter and latency-sensitive applications (see QoS (Quality of Service) Parameters (BSU Only) for details on configuration). This field is inactive and makes no difference whether is enabled or disabled.
- **Automatic Multi-Frame Bursting:** In order to achieve higher throughput, WORP protocol allows each side (BSU or SU) to send a burst of up to 4 data messages instead of a single data message. The sole criteria for sending a burst is enough traffic to be sent out. This feature is called Multi-Frame Bursting support.

  Automatic Multi-Frame bursting optimizes multi-burst performance when configuring QoS high-priority Service Flows. Three scenarios may be defined:

  – *No Multi-Frame Burst Support* –To disable Multi-Frame burst support, click **Configure** > **Network** > **Roaming,** and select “Disable” on the drop-down box (see BSU Roaming Configuration). In this case, each active SFC is limited to send a single data message. Total throughput available to the remaining best effort traffic is around 76% of the maximum available throughput.

  – *Multi-Frame Burst Support* – The system will enable Multi-Frame burst for *all* SFCs, but the maximum number of data messages sent in a burst will be defined by the parameter “Number of data messages in a burst” for each of the SFCs (see Service Flow Class (SFC)). This scenario is set by clicking **Configure** > **Network** > **Roaming** and enabling Multi-Frame burst on the drop-down box (see BSU Roaming Configuration), and disabling **Automatic Multi-Frame Bursting** (this parameter).

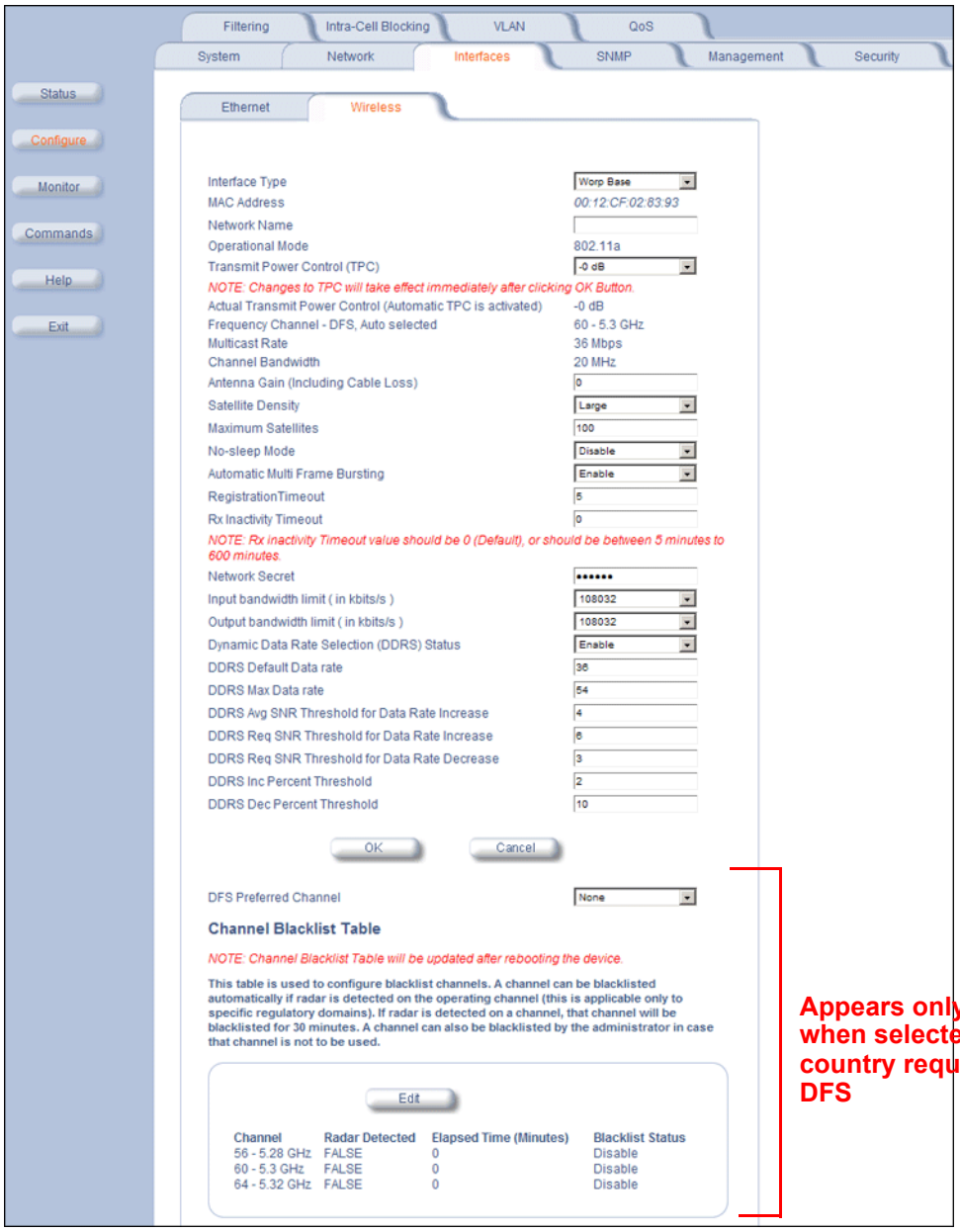
    The maximum number of data messages in a burst directly influences the total throughput of the system. Typical values are:

No. of messages in a burst:	% of the maximum throughput:
4	100%
3	97.6%
2	92.9%
1	76.2%

  – *Automatic Multi-Frame Burst Support* – The system will continuously monitor which of the active SFCs has the highest priority and dynamically enable Multi-Frame burst for the highest priority SFC only, keeping all the lower priority SFCs with Multi-Frame burst disabled. If there are multiple SFCs having the same, highest priority, all of them will have Multi-Frame burst enabled. The maximum number of data messages sent in a burst is defined by the parameter “Number of data messages in a burst” and it can be different for each SFC (see Service Flow Class (SFC)). This scenario is set by clicking **Configure** > **Network** > **Roaming** and enabling Multi-Frame burst on the drop-down box (see BSU Roaming Configuration), and enabling **Automatic Multi-Frame Bursting** (this parameter). In this case, even the lowest priority SFC will have Multi-Frame burst dynamically enabled as long as it is the only SFC in the system that has traffic. By default, configuring even a single high priority SFC with automatic multi-frame bursting enabled will decrease throughput of low priority best-effort traffic to approximately 76% of maximum available throughput, because low priority traffic will have Multi-Frame burst disabled to optimize bandwidth for the high priority traffic.
- **Registration Timeout:** This is the registration process time-out of an SU on a BSU. Default is 5 seconds.
- **Rx Inactivity Timeout:** This is the activity time-out of an SU on a BSU. If no traffic is received on the WORP interface in the configured time, the unit will reboot. The range is 5 minutes to 600 minutes.
- **Network Secret:** A network secret is a secret password given to all nodes of a network. An SU can only register to a BSU if it has the same Network Secret. The Network Secret is sent encrypted and can be used as a security option.
- **Input / Output Bandwidth Limit:** These parameters limit the data traffic received on the wireless interface and transmitted to the wireless interface, respectively. Selections are in steps of 64 Kbps from 64 Kbps to 108,064 Kbps.
- **Dynamic Data Rate Selection (DDRS) Status:** Select the **DDRS Status** “Enable” or “Disable” from the drop-down box provided. When you enable or disable DDRS on the BSU, the BSU sends an announcement to the SUs and the SUs enable or disable DDRS automatically.

- **DDRS Default Data Rate:** The data rate at which the BSU starts communication with all SUs to begin the registration process (the default is 6 Mbps). This data rate is configured on the BSU only.
- **DDRS Max Data Rate:** When DDRS is enabled, configure the maximum data rate that can be dynamically set by DDRS.
- **DDRS Avg SNR Threshold for Data Rate Increase:** This field is displayed only when DDRS is enabled. The current remote SNR value must be bigger than average remote SNR value by at least this threshold in dB, in order the DDRS to increase the TX data rate.
- **DDRS Req SNR Threshold for Data Rate Increase:** The average remote SNR value must be bigger than or equal to the minimum required SNR value for the higher TX data rate by at least this threshold in dB in order for DDRS to increase the TX data rate to the higher TX data rate.
- **DDRS Avg SNR Threshold for Data Rate Decrease:** The average remote SNR must be less than the minimum required SNR for the current TX data rate by at least this threshold in dB, in order for DDRS to decrease the TX data rate.
- **DDRS Inc Percent Threshold:** If the number of retransmissions out of the last 128 transmissions is bigger than this percentage, DDRS will increase the TX data rate.
- **DDRS Dec Percent Threshold:** If the number of retransmissions out of last 128 transmissions is less than or equal to this percentage, DDRS will decrease the TX data rate.

Additionally, the BSU screen for countries that require DFS contains the sections described below.



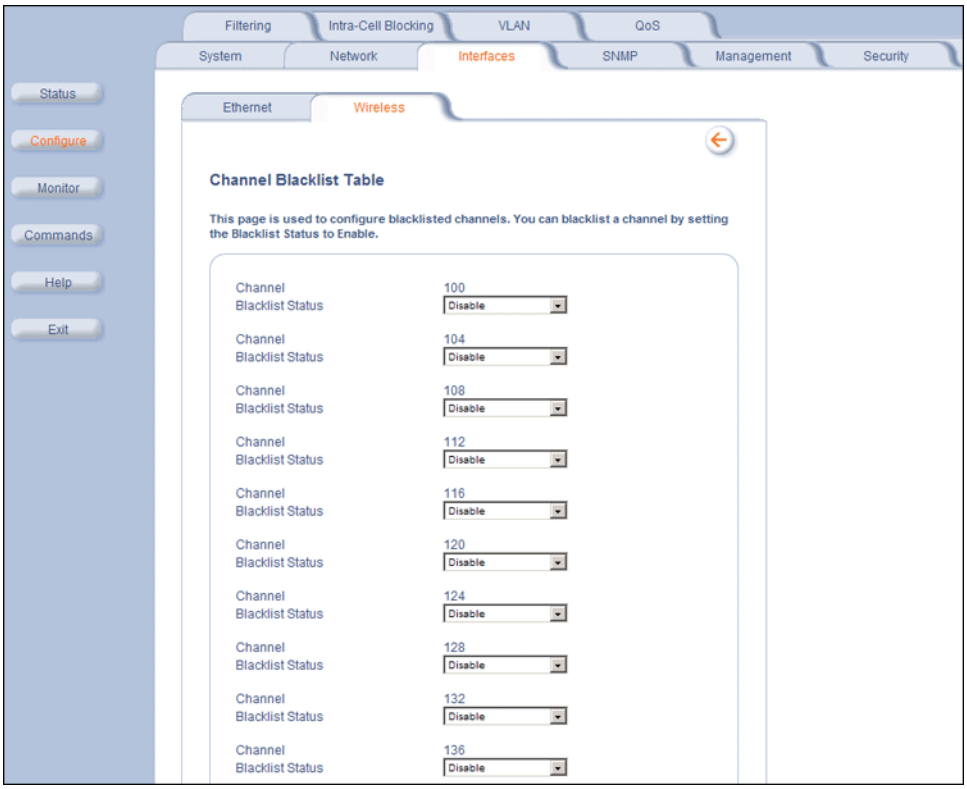
- **DFS Preferred Channel:** A single DFS preferred frequency channel on the BSU is provided so that when the DFS process starts the BSU will first try the DFS preferred channel before scanning all the other active channels in the DFS channel list. The DFS preferred channel must be selected from those channels indicated as “Disable” in the DFS channel blacklist list. It is not possible to select the DFS preferred channel from those channels in the DFS channel blacklist list indicated as “Enable”.
- **Channel Blacklist Table:** The DFS channel blacklist table shows all the channels in the current bandwidth and specifies the blacklist status of each channel as one of the following:
  - Enable: Channels that are made unavailable either for a certain period of time upon detection of a radar signal, or permanently because the operator has configured them as blacklisted. These channels are skipped over during DFS channel selection.
  - Disable: Channels that are to be scanned during DFS.

Edit Entries to the Channel Blacklist Table

In accordance with ETSI, IC, and FCC non-occupancy rules, when interference is detected on any active channel, that channel will be blacklisted. The channel will not be used for a period of 30 minutes after the interference has been detected. The elapsed time is also shown in the DFS channel blacklist table. When the elapsed time for a channel in the blacklist is greater than or equal to 30 minutes, the blacklist status of the channel will change to Disable.

If an operator knows in advance on which channels interference is likely to exist, those channels can be blacklisted and hence they will be skipped during DFS. Similarly, if the operator knows of channels where interference is unlikely to be detected, those channels can be defined as active and hence they will be scanned during DFS. This makes the process more efficient.

When you click **Edit**, the channel blacklist table screen appears. Here you can manually configure each channel as “active” (Blacklist Status = Disable) or “blacklisted” (Blacklist Status = Enable). Enter your changes and click **OK**. To go back, click on the arrow button.

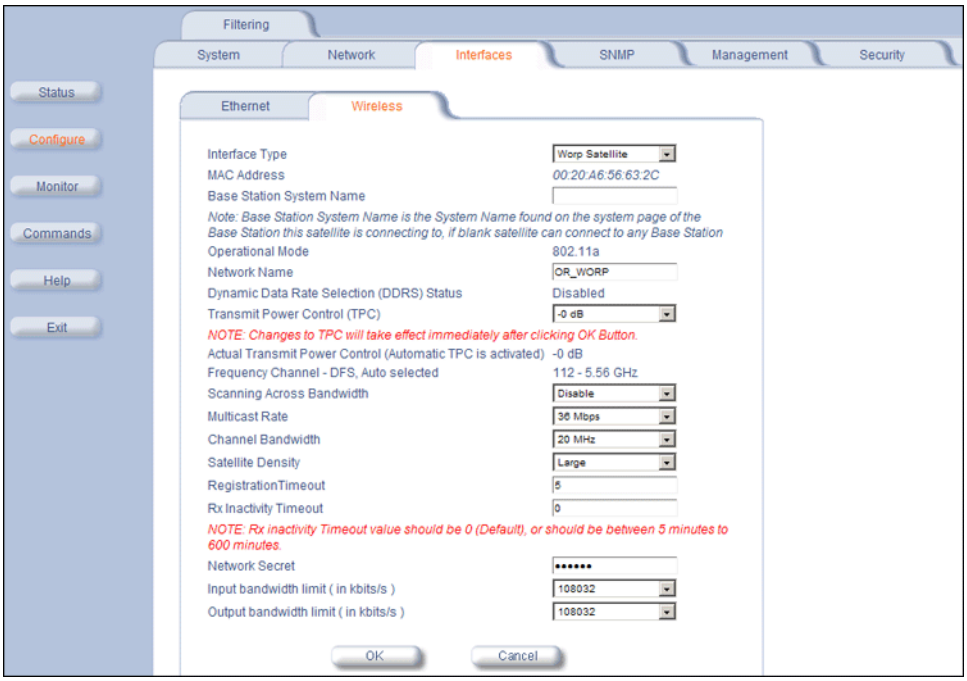


Satellite Mode

The mandatory parameters to configure for registration of the SU on a Base Station are:

- Network Name
- Base Station System Name (when used)
- Channel Frequency
- Encryption (when used)
- Network Secret

These and other parameters found on the SU's **Interfaces > Wireless** page are described below.



- **Interface Type:** In Satellite mode, the interface type is **WORP Satellite**.
- **MAC Address:** The factory-assigned MAC address of the unit. This is a read-only field.
- **Base Station System Name:** The name found on the system page of the BSU to which this SU is connecting. This parameter can be used as an added security measure, and when there are multiple BSUs in the network and you want an SU to register with only one when it may actually have adequate signal strength for either. The System Name field is limited to a length of 32 bytes.

  If the Base Station System Name is left blank on the SU, it can register with any BSU with a matching Network Name and Network Secret.
- **Operational Mode:** This field indicates the operational mode of the unit, depending upon the specific Tsunami MP.11. This operational mode cannot be changed as it is based upon a license file.
- **Network Name:** A Network Name is a name given to a network so that multiple networks can reuse the same frequency without problems. An SU can only register to its base if it has the same Network Name. The Network Name is one of the parameters that allow a Subscriber Unit to register on a Base Station. The **Base Station System Name** and **Frequency Channel** also are parameters to guide the SU to the proper BSU on the network, but they provide no security. Basic security is provided through encryption, as it causes none of the messages to be sent in the clear. Further security is provided by mutual authentication of the BSU and SU using the **Network Secret**. The Network Name can be 2 to 32 characters in length.
- **Dynamic Data Rate Selection (DDRS) Status:** For the **WORP Satellite Mode**, **DDRS Status** is read-only parameter and its value is based upon the **WORP Base** to which this SU is associated.

- **Transmit Power Control (TPC):** By default, the unit lets you transmit at the maximum output power for the country/band or regulatory domain and frequency selected. However, with Transmit Power Control (TPC), you can adjust the output power of the unit to a lower level in order to reduce interference to neighboring devices or to use a higher gain antenna without violating the maximum radiated output power allowed for your country/band. Also, some countries/bands that require DFS also require the transmit power to be set to a 6 dB lower value than the maximum allowed EIRP when link quality permits. You can see your unit's current output power for the selected frequency in the event log.

  The event log shows the selected power for all data rates, so you must look up the proper data rate to determine the actual power level.

  NOTE: *This feature only lets you decrease your output power; it does not let you increase your output power beyond the maximum allowed defaults for your frequency and country.*

  Select one of the following options and click **OK** at the bottom of the window. Your original output power is adjusted relative to the value selected. The new setting takes effect immediately without rebooting:

TPC Selection (dB)	Maximum TX Power (dBm)
0 (default)	16
-3	13
-6	10
-9	7
-12	4
-15	1
-18 (minimum TPC level)	0

  NOTE: *24 Mbps and lower modulation have maximum +16 dBm TX power, 36 Mbps has maximum +13 dBm TX power, 48 Mbps has maximum +12 dBm TX power, and 54 Mbps has maximum +11 dBm TX power. Because higher modulation has a lower maximum TX power, the total TPC range is smaller at a higher data rate. Because the minimum TX power is equal for all data rates, each TPC selection has constant TX power for all data rates except where the maximum TX power is limited.*

- **Actual Transmit Power Control:** This field displays the actual transmit power when ATPC is enabled.
- **Enable Turbo Mode *(Non-DFS US Only)*:** Check this box to enable Turbo Mode. **Turbo Mode is supported only in the United States when DFS is not required.** Enabling turbo mode, in its current implementation, allows the unit to use two adjacent frequency channels to transmit and receive a signal. By enabling turbo mode, the receive sensitivity improves by 4 dB for the 36 Mbps data rate and by 2 dB for the 24 Mbps data rate.

  NOTE: *The additional sensitivity is provided with the impact of using twice as much spectrum and thus increasing the opportunity of interference and decreased ability for system collocation. Generally, Turbo mode is not recommended except when the extra sensitivity is absolutely required.*

- **Frequency Channel:** The frequency channel indicates the band center frequency the unit uses for communicating with peers. This frequency channel can be set in several ranges, depending upon regulatory domain. Refer to Country Codes and Channels for channelization information. For countries in which DFS is not required, the **Frequency Channel** list displays only the channels and frequencies allowed for the selected country/band.

  For countries/bands in which DFS is required, **Frequency Channel** is not configurable. Instead the channel is auto-selected by the DFS process.
- **Scanning Across Bandwidth:** As the 5054 (MP.11a) supports only 20 MHz operation, this parameter has no effect.
- **Multicast Rate:** The rate at which data is to be transferred. This drop down box is unavailable when DDRS is enabled.

  The default multicast rate for the unit is 36 Mbps. The SU must never be set to a lower data rate than the BSU because timeouts will occur at the BSU and communication will fail.

  Selections for multicast rate are shown in the following table:

Multicast Rates in Mbps	Multicast Rates in Mbps with Turbo Mode Enabled (Non-DFS US Only)
6	12
9	18
12	24
18	36
24	48
36	72
48	96
54	108

- **Channel Bandwidth:** This is a read only field. Channel Bandwidth is set at 20 MHz.
- **Satellite Density:** The **Satellite Density** setting is a valuable feature for achieving maximum bandwidth in a wireless network. It influences the receive sensitivity of the radio interface and improves operation in environments with a high noise level. Reducing the sensitivity of the unit enables unwanted “noise” to be filtered out (it disappears under the threshold).

  You can configure the **Satellite Density** to be **Large**, **Medium**, **Small**, **Mini**, or **Micro**. The default value for this setting is Large. The smaller settings are appropriate for high noise environments; a setting of **Large** would be for a low noise environment.

  A long distance link may have difficulty maintaining a connection with a small density setting because the wanted signal can disappear under the threshold. Consider both noise level and distance between the peers in a link when configuring this setting. The threshold should be chosen higher than the noise level, but sufficiently below the signal level. A safe value is 10 dB below the present signal strength.

  If the Signal-to-Noise Ratio (SNR) is not sufficient, you may need to set a lower data rate or use antennas with higher gain to increase the margin between wanted and unwanted signals. In a point-to-multipoint configuration, the BSU should have a density setting suitable for all of its registered SUs, especially the ones with the lowest signal levels (longest links).

  Take care when configuring a remote interface; check the available signal level first, using Remote Link Test.

  WARNING: When the remote interface accidentally is set at too small a value and communication is lost, it cannot be reconfigured remotely and a local action is required to bring the communication back. Therefore, the best place to experiment with the level is at the unit that can be managed without going through the link; if the link is lost, the setting can be adjusted to the correct level to bring the link back.

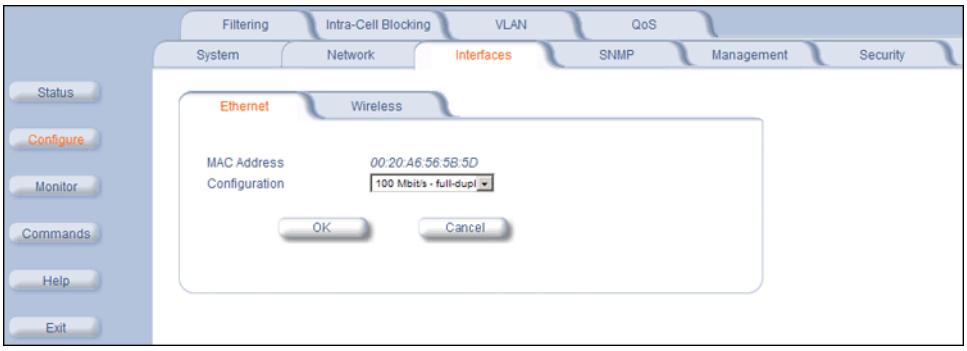
  Sensitivity threshold settings related to the density settings for the unit are:

Satellite Density:	Receive Sensitivity Threshold	Defer Threshold
Large	-95 dBm	-62 dBm
Medium	-86 dBm	-62 dBm
Small	-78 dBm	-52 dBm
Mini	-70 dBm	-42 dBm
Micro	-62 dBm	-36 dBm

- **Registration Timeout:** This is the registration process time-out of an SU on a BSU. Default is 5 seconds.
- **Rx Activity Timeout:** This is the activity time-out of an SU on a BSU. Default is 0 seconds.
- **Network Secret:** A network secret is a secret password given to all nodes of a network. An SU can only register to a BSU if it has the same Network Secret. The Network Secret is sent encrypted and can be used as a security option.
- **Input / Output Bandwidth Limit:** These parameters limit the data traffic received on the wireless interface and transmitted to the wireless interface, respectively. Selections are in steps of 64 Kbps from 64 Kbps to 108,064 Kbps.

Ethernet

To set the Ethernet speed, duplex mode, and input and output bandwidth limits, click **Configure** > **Interfaces** > **Ethernet**.



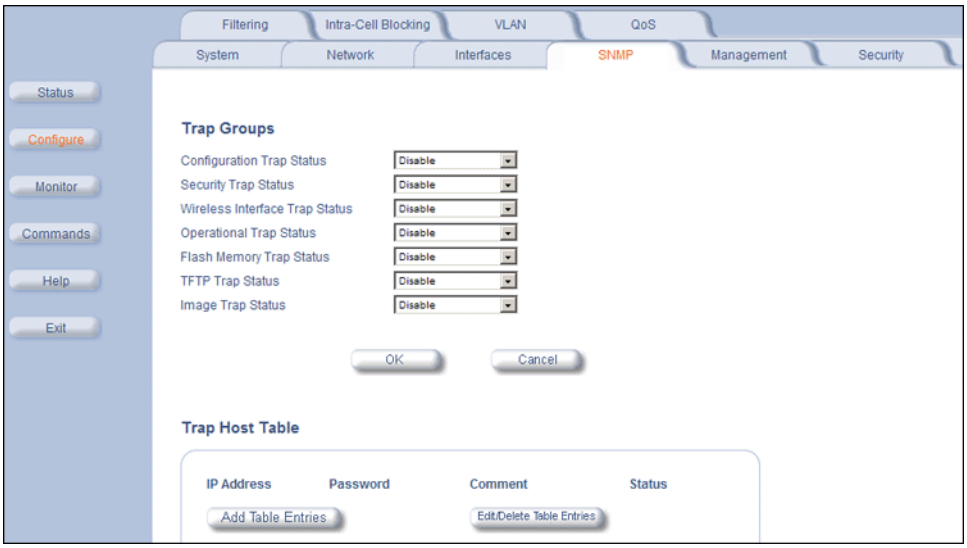
You can set the desired speed and transmission mode by clicking on **Configuration**. Select from these settings for the type of Ethernet transmission:

- **Half-duplex** means that only one side can transmit at a time.
- **Full-duplex** lets both sides transmit.
- **Auto-duplex** selects the best transmission mode available when both sides are set to auto-select.

The recommended setting is **auto-speed-auto-duplex**.

SNMP Parameters

Click **Configure** > **SNMP** to enable or disable trap groups, and to configure the SNMP management stations to which the unit sends system traps. See “Trap Groups” in the *Tsunami MP.11/QB.11 Reference Manual* for a list of the system traps.

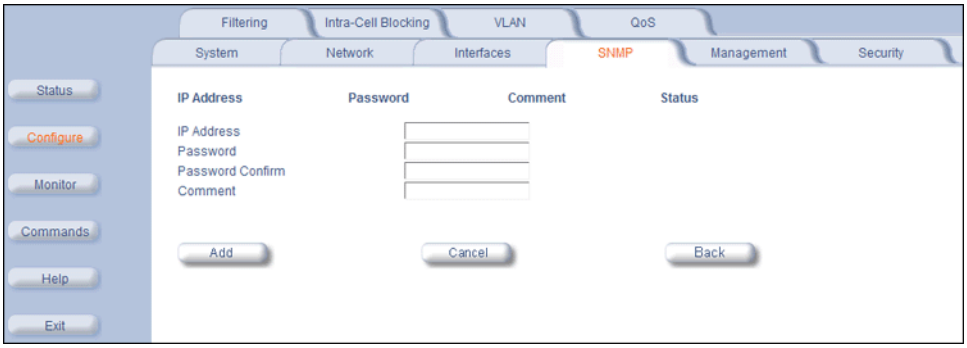


- **Trap Groups:** You can enable or disable different types of traps in the system. By default, all traps are enabled.
- **Trap Host Table:** This table shows the SNMP management stations to which the unit sends system traps.

Trap Host Table

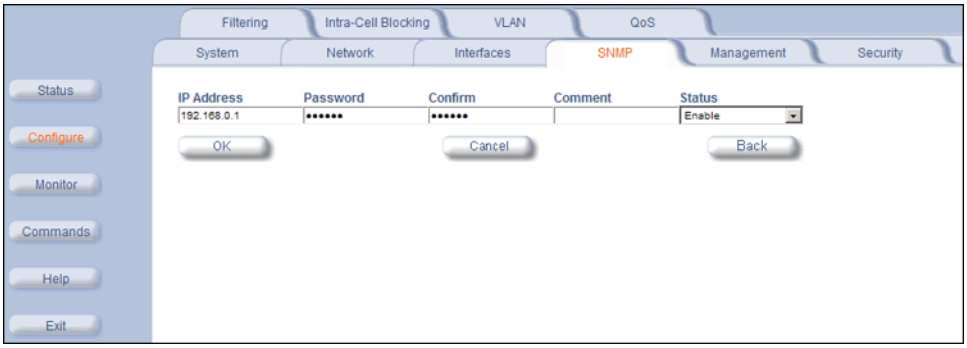
Add Entries to the Trap Host Table

Click the **Add Table Entries** button to add entries to the Trap Host Table.



Edit/Delete Entries in the Trap Host Table

Click the **Edit/Delete Table Entries** button to make changes to or delete existing entries.

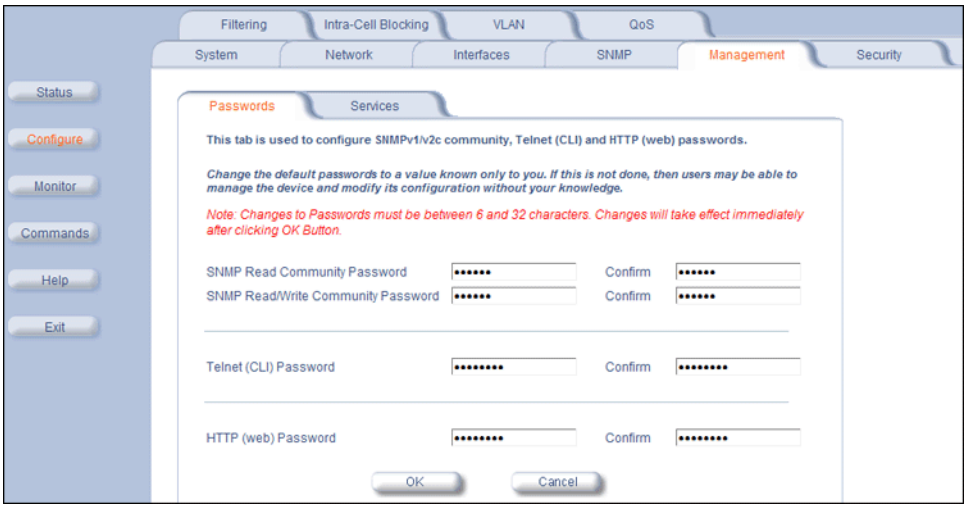

Filtering
Intra-Cell Blocking
VLAN
QoS
System
Network
Interfaces
SNMP
Management
Security
Status
Configure
Monitor
Commands
Help
Exit
IP Address
Password
Confirm
Comment
Status
192.168.0.1
Enable
OK
Cancel
Back

Management Parameters

Use the Management tab to configure passwords and other service parameters.

Passwords

The **Password** tab lets you configure the SNMP, Telnet, and HTTP (Web Interface) passwords.

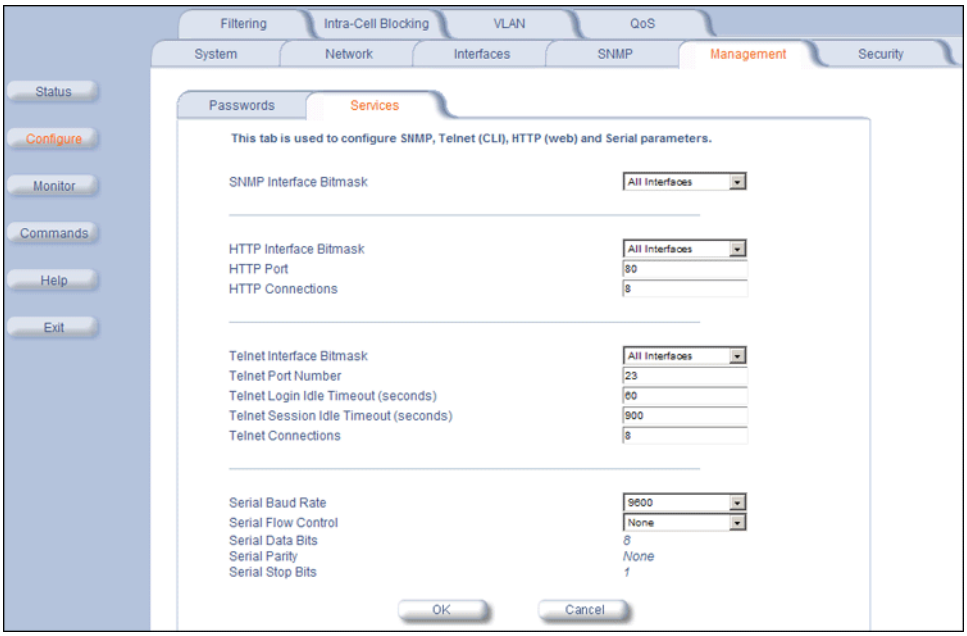


For all password fields, the passwords must be between 6 and 32 characters. Changes take effect immediately after you click **OK**. The following passwords are configurable:

- **SNMP Read Community Password:** The password for read access using SNMP. Enter a password in both the **Password** field and the **Confirm** field. The default password is **public**.
- **SNMP Read/Write Community Password:** The password for read and write access using SNMP. Enter a password in both the **Password** field and the **Confirm** field. The default password is **public**.
- **Telnet (CLI) Password:** The password for the CLI interface. Enter a password in both the **Password** field and the **Confirm** field. The default password is **public**.
- **HTTP (Web) Password:** The password for the Web browser HTTP interface. Enter a password in both the **Password** field and the **Confirm** field. The default password is **public**.

Services

The **Services** tab lets you configure the SNMP, Telnet, HTTP (Web Interface), and serial connection parameters. Changes to these parameters require a reboot to take effect.



SNMP Configuration Settings

- **SNMP Interface Bitmask:** Configure the interface or interfaces (**All Interfaces, Only Ethernet**, **Only Slot A, None**) from which you will manage the unit using SNMP. You also can select **Disabled** to prevent a user from accessing the unit through SNMP.

HTTP Configuration Settings

- **HTTP Interface Bitmask:** Configure the interface or interfaces (**All Interfaces, Only Ethernet**, **Only Slot A, None**) from which you will manage the unit through the Web interface. For example, to allow Web configuration through the Ethernet network only, set **HTTP Interface Bitmask** to **Ethernet**. You can also select **Disabled** to prevent a user from accessing the unit from the Web interface.
- **HTTP Port:** Configure the HTTP port from which you will manage the unit through the Web interface. By default, the HTTP port is 80.
- **HTTP Connections**: The number of allowed HTTP connections (the maximum is 8).

Telnet Configuration Settings

NOTE: *To use HyperTerminal for CLI access, make sure to check "Send line ends with line feeds" in the ASCII Setup window (in the HyperTerminal window, click Properties; then select Setup > ASCII Setup. See "HyperTerminal Connection Properties" in the Tsunami MP.11/QB.11 Reference Manual for more information).*

- **Telnet Interface Bitmask:** Select the interface (Ethernet, Wireless, All Interfaces) from which you can manage the unit through telnet. This parameter can also be used to disable telnet management.
- **Telnet Port Number:** The default port number for Telnet applications is 23. However, you can use this field if you want to change the Telnet port for security reasons (but your Telnet application also must support the new port number you select).
- **Telnet Login Timeout** (seconds): Enter the number of seconds the system is to wait for a login attempt. The unit terminates the session when it times out. The range is 1 to 300 seconds; the default is 30 seconds.
- **Telnet Session Timeout** (seconds): Enter the number of seconds the system is to wait during a session while there is no activity. The unit ends the session upon timeout. The range is 1 to 36000 seconds; the default is 900 seconds.
- **Telnet Connections**: The number of allowed Telnet connections (the maximum is 8).

Serial Configuration Settings

The serial port interface on the unit is enabled at all times. See “Serial Port” in the *Tsunami MP.11/QB.11 Reference Manual* for information about how to access the CLI interface through the serial port. You can configure and view following parameters:

- **Serial Baud Rate:** Select the serial port speed (bits per second). Choose between 2400, 4800, 9600, 19200, 38400, or 57600; the default Baud Rate is 9600.
- **Serial Flow Control:** Select either None (default) or Xon/Xoff (software controlled) data flow control. To avoid potential problems when communicating with the unit through the serial port, Proxim recommends that you leave the Flow Control setting at None (the default value).
- **Serial Data Bits:** This is a read-only field and displays the number of data bits used in serial communication (8 data bits by default).
- **Serial Parity:** This is a read-only field and displays the number of parity bits used in serial communication (no parity bits by default).
- **Serial Stop Bits:** This is a read-only field that displays the number of stop bits used in serial communication (1 stop bit by default).

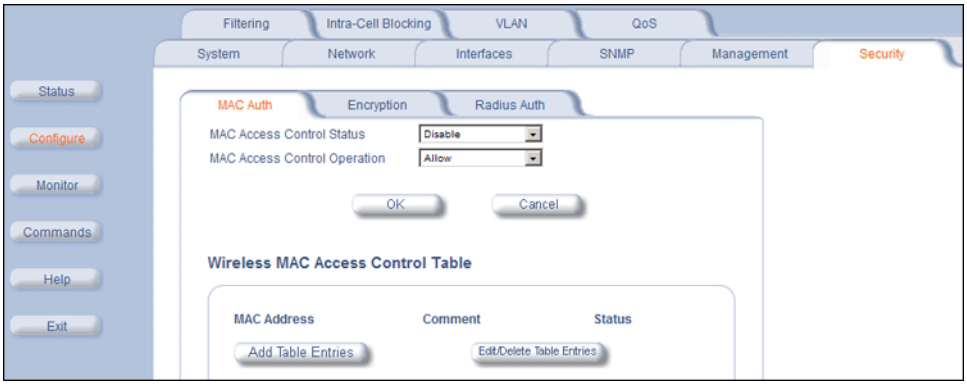
The serial port bit configuration is commonly referred to as 8N1.

Security Parameters

MAC Authentication (BSU Only)

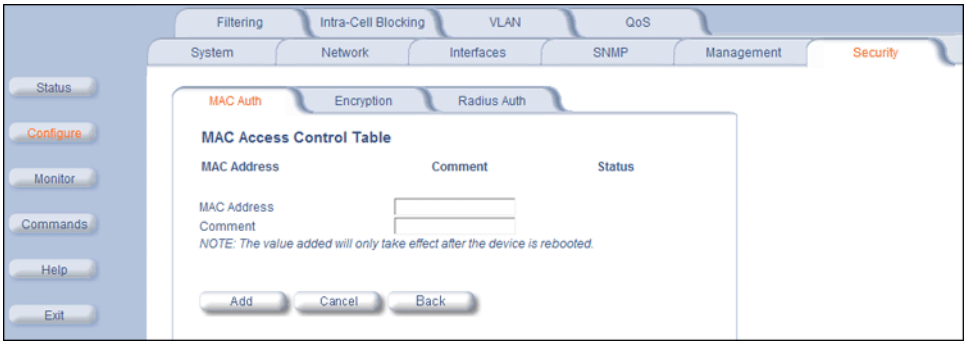
Click **Configure** > **Security** > **MAC Auth** to build a list of authorized wireless stations that can register at the unit and access the network. MAC Authentication is supported on the wireless interface and only wireless MAC addresses should be entered in the list. For example, you might build a list of wireless MAC addresses of SUs authorized on the BSU

NOTE: *MAC authentication is available only for BSUs.*



Add Entries to MAC Access Control Table

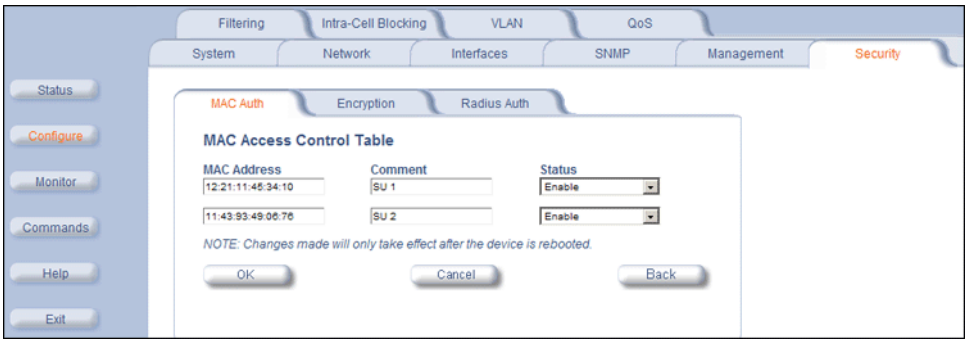
1. To add table entries, click the **Add Table Entries** button; the following screen will be displayed:



2. Enter the MAC address and any comment, then click **Add**. The maximum number of MAC addresses that can be entered is 250.

Edit/Delete Entries in MAC Access Control Table

1. To edit or delete table entries, click the **Edit/Delete Table Entries** button
2. Make your corrections in the window displayed and click **OK**.



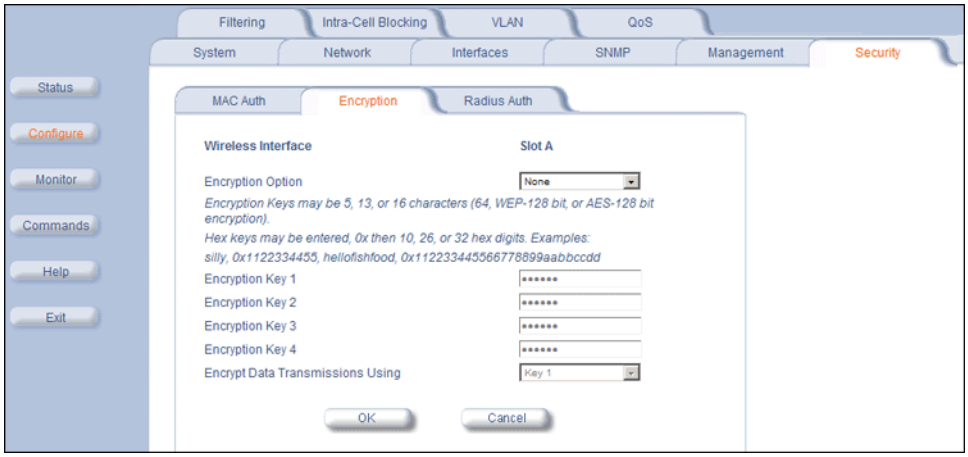
Encryption

NOTE: *Be sure to set the encryption parameters and change the default passwords.*

You can protect the wireless data link by using encryption. In addition to Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP), the unit supports Advanced Encryption Standard (AES) 128-bit encryption. To provide even stronger encryption, the AES CCM Protocol is also supported.

Encryption keys can be 5 (64-bit), 13 (WEP 128-bit), or 16 (AES 128-bit) characters in length. Both ends of the wireless data link must use the same parameter values.

Click **Configure** > **Security** > **Encryption** to set encryption keys for the data transmitted and received by the unit. Note that all devices in one network must use the same encryption parameters to communicate to each other.

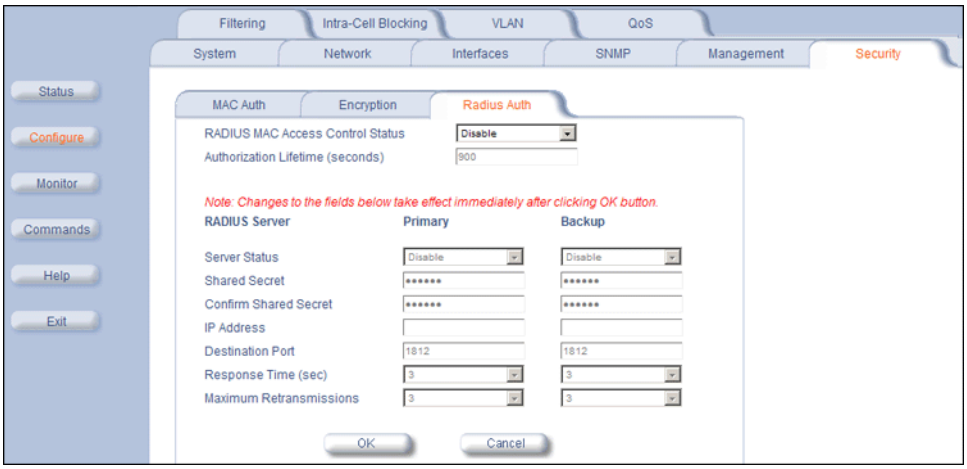


RADIUS Authentication (BSU Only)

In large networks with multiple units, you can maintain a list of MAC addresses on a centralized location using a RADIUS authentication server that grants or denies access. If you use this kind of authentication, you must specify at least the primary RADIUS server. The backup RADIUS server is optional.

Click **Configure** > **Security** > **Radius Auth** to set the IP address of the RADIUS server containing the central list of MAC addresses that are allowed to access the network. The RADIUS parameters let you enable HTTP or Telnet RADIUS management access to configure a RADIUS Profile for management access control, to enable or disable local user access, and to configure the local password.

NOTE: *RADIUS authentication is available only for BSUs.*


Filtering
Intra-Cell Blocking
VLAN
QoS
System
Network
Interfaces
SNMP
Management
Security
Status
Configure
Monitor
Commands
Help
Exit
MAC Auth
Encryption
Radius Auth
RADIUS MAC Access Control Status
Disable
Authorization Lifetime (seconds)
900
Note: Changes to the fields below take effect immediately after clicking OK button.
RADIUS Server
Primary
Backup
Server Status
Disable
Disable
Shared Secret
Confirm Shared Secret
IP Address
Destination Port
1812
1812
Response Time (sec)
3
3
Maximum Retransmissions
3
3
OK
Cancel

Filtering Parameters

Overview

Click **Configure** > **Filtering** to configure packet filtering. Packet filtering can be used to control and optimize network performance.

The Filtering feature can selectively filter specific packets based upon their Ethernet protocol type. Protocol filtering is done at the Bridge layer.

Protocol filters are useful for preventing bridging of selected protocol traffic from one segment of a network to other segments (or subnets). You can use this feature both to increase the amount of bandwidth available on your network and to increase network security.

Increasing Available Bandwidth

It may be unnecessary to bridge traffic from a subnet using IPX/SPX or AppleTalk to a segment of the network with UNIX workstations. By denying the IPX/SPX AppleTalk traffic from being bridged to the UNIX subnet, the UNIX subnet is free of this unnecessary traffic.

Increasing Network Security

By bridging IP and IP/ARP traffic and blocking LAN protocols used by Windows, Novell, and Macintosh servers, you can protect servers and client systems on the private local LAN from outside attacks that use those LAN protocols. This type of filtering also prevents private LAN data from being bridged to an untrusted remote network or the Internet.

To prevent blocking your own access (administrator) to the unit, Proxim recommends that IP (0x800) and ARP (0x806) protocols are always passed through.

Sample Use and Validation

Configure the protocol filter to let only IP and ARP traffic pass through the unit (bridge) from one network segment to another. Then, attempt to use Windows file sharing across the bridge. The file should not allow sharing; the packets are discarded by the bridge.

Setting the ARP Filter

There may be times when you need to set the ARP or Multicast. Usually, this is required when there are many nodes on the wired network that are sending ARP broadcast messages or multicast packets that unnecessarily consume the wireless bandwidth. The goal of these filters is to allow only necessary ARP and multicast traffic through the 1.6 Mbps wireless pipe.

The TCP/IP Internet Protocol Suite uses a method known as ARP (Address Resolution Protocol) to match a device's MAC (Media Access Control) address with its assigned IP address. The MAC address is a unique 48-bit identifier assigned to each hardware device at the factory by the manufacturer. The MAC address is commonly represented as 6 pairs of hexadecimal digits separated by colons. For example, a device may have the MAC address of 00:20:A6:33:ED:45.

When devices send data over the network (Ethernet, Token Ring, or wireless), they use the MAC address to identify a packet's source and destination. Therefore, an IP address must be mapped to a MAC address in order for a device to send a packet to particular IP address. In order to resolve a remote node's IP address with its MAC address, a device sends out a broadcast packet to all nodes on the network. This packet is known as an ARP request or ARP broadcast and requests that the device assigned a particular IP address respond to the sender with its MAC address.

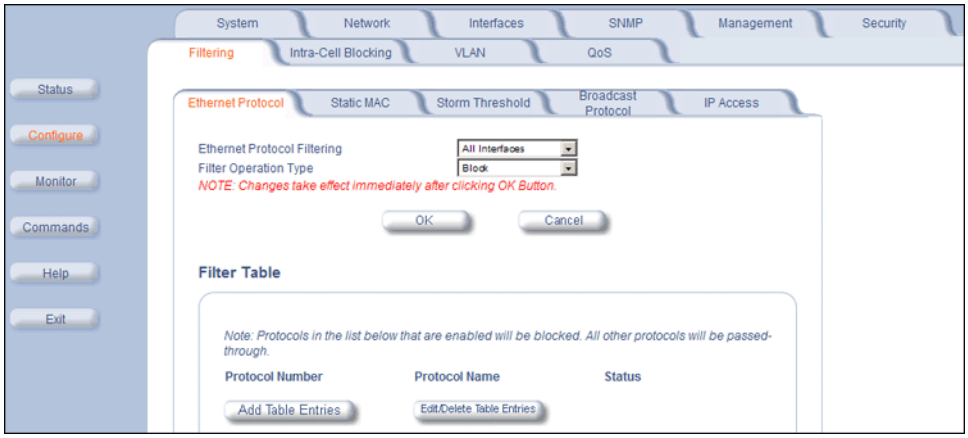
Because ARP requests are broadcast packets, these packets are forwarded to wireless nodes by default, even if the packet is not meant for a wireless node. As the number of nodes on a network backbone increases, so does the number of ARP broadcasts that are forwarded to the wireless nodes. Many of these ARP broadcasts are unnecessary and can

consume valuable wireless bandwidth. On some networks, there are so many ARP broadcasts that the performance of the wireless network will degrade due to the amount of bandwidth being consumed by these messages.

To reduce the number of ARP broadcasts that are forwarded to the wireless nodes, you can enable ARP filtering. When enabled, the ARP Filter allows the unit to forward only those ARP broadcasts destined for an IP address that falls within the range specified by the ARP Filter Network Address and the ARP Filter Subnet Mask. The ARP Filter performs a logical AND function (essentially keeping what is the same and discarding what is different) on the IP address of the ARP request and the ARP Filter Subnet Mask. It then compares the result of the logical AND to the ARP Filter Network Address. If the two values match, the ARP broadcast is forwarded to the wireless network by the unit.

Ethernet Protocol

The Ethernet Protocol filter blocks or forwards packets based upon the Ethernet protocols they support. Click **Configure** > **Filtering** > **Ethernet Protocol** to enable or disable certain protocols in the table. Entries can be selected from a drop-down box.



Follow these steps to configure the Ethernet Protocol Filter:

1. Select the interfaces that will implement the filter from the **Ethernet Protocol Filtering** drop-down menu.
   - Ethernet: Packets are examined at the Ethernet interface
   - Wireless-Slot A or Wireless-Slot B: Packets are examined at the Wireless A or B interfaces
   - All Interfaces: Packets are examined at both interfaces
   - Disabled: The filter is not used
2. Select the **Filter Operation Type**.
   - If set to Block, the bridge blocks enabled Ethernet Protocols listed in the Filter Table.
   - If set to Passthru, only the enabled Ethernet Protocols listed in the Filter Table pass through the bridge.
3. Configure the **Filter Table**. See below.

   NOTE: *Entries must be enabled in order to be subject to the filter.*

Add Entries to the Filter Table

1. Click **Add Table Entries.** You may add one of the supplied Ethernet Protocol Filters, or you may enter additional filters by specifying the appropriate parameters:
   - To add one of the supplied Ethernet Protocol Filters to the filter table:
     – Select the appropriate filter from the **Specify Common Protocol** drop-down menu. Protocol Name and Protocol Number fields will be filled in automatically.
     – Click **Add**
   - To add a new filter to the filter table:

– Enter the **Protocol Number**. See http://www.iana.org/assignments/ethernet-numbers for a list of protocol numbers.
– Enter the Protocol Name.
– Click **Add**.

Edit/Delete Entries in the Filter Table

1. Click **Edit** and change the information, or select Enable, Disable, or Delete from the Status drop-down menu.

Static MAC Address Filtering

Overview

The Static MAC Address filter optimizes the performance of a wireless (and wired) network. When this feature is configured properly, the unit can block traffic between wired devices on the wired (Ethernet) interface and devices on the wireless interface based upon MAC address.

NOTE: *The device on the wireless interface can be any device connected through the link. It can be directly connected to the Ethernet interface of the peer unit, or it can be attached through multiple hops. The MAC address in the packets arriving at the wireless interface is the important element.*

The filter is an advanced feature that lets you limit the data traffic between two specific devices (or between groups of devices based upon MAC addresses and masks) through the unit's wireless interface. For example, if you have a server on your network with which you do not want wireless clients to communicate, you can set up a static MAC filter to block traffic between these devices. The Static MAC Filter Table performs bi-directional filtering. However, note that this is an advanced filter and it may be easier to control wireless traffic through other filter options, such as **Protocol Filtering**.

Each MAC address or mask is comprised of 12 hexadecimal digits (0-9 and A-F) that correspond to a 48-bit identifier. Each hexadecimal digit represents 4 bits (0 or 1).

Taken together, a MAC address/mask pair specifies an address or a range of MAC addresses that the unit looks for when examining packets. The unit uses Boolean logic to perform an "and" operation between the MAC address and the mask at the bit level. However, for most users, you do not need to think in terms of bits. It should be sufficient to create a filter using only the hexadecimal digits 0 and F in the mask (where 0 is any value and F is the value specified in the MAC address). A mask of 00:00:00:00:00:00 corresponds to all MAC addresses, and a mask of FF:FF:FF:FF:FF:FF:FF:FF applies only to the specified MAC address.

For example, if the MAC address is 00:20:A6:12:54:C3 and the mask is FF;FF;FF;00:00:00, the unit examines the source and destination addresses of each packet looking for any MAC address starting with 00:20:A6. If the mask is FF;FF;FF;FF;FF;FF, the unit looks only for the specific MAC address (in this case, 00:20:A6:12:54:C3).

When creating a filter, you can configure the Wired parameters only, the Wireless parameters only, or both sets of parameters. Which parameters to configure depends upon the traffic that you want to block:

- To prevent all traffic from a specific wired MAC address from being forwarded to the wireless network, configure only the Wired MAC address and Wired mask (leave the Wireless MAC and Wireless mask set to all zeros).
- To prevent all traffic from a specific wireless MAC address from being forwarded to the wired network, configure only the Wireless MAC and Wireless mask (leave the Wired MAC address and Wired mask set to all zeros).
- To block traffic between a specific wired MAC address and a specific wireless MAC address, configure all four parameters.

See Static MAC Filter Examples for more detailed examples.

Static MAC Filter Examples

Consider a network that contains a wired server and three wireless clients. The MAC address for each unit is as follows:

- **Wired Server:** 00:40:F4:1C:DB:6A
- **Wireless Client 1:** 00:02:2D:51:94:E4
- **Wireless Client 2:** 00:02:2D:51:32:12
- **Wireless Client 3:** 00:20:A6:12:4E:38

Prevent Two Specific Devices from Communicating

Configure the following settings to prevent the Wired Server and Wireless Client 1 from communicating:

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:02:2D:51:94:E4
- **Wireless Mask:** FF:FF:FF:FF:FF:FF

Result: Traffic between the Wired Server and Wireless Client 1 is blocked. Wireless Clients 2 and 3 still can communicate with the Wired Server.

Prevent Multiple Wireless Devices From Communicating With a Single Wired Device

Configure the following settings to prevent Wireless Clients 1 and 2 from communicating with the Wired Server:

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:02:2D:51:94:E4
- **Wireless Mask:** FF:FF:FF:00:00:00

Result: When a logical “AND” is performed on the Wireless MAC Address and Wireless Mask, the result corresponds to any MAC address beginning with the 00:20:2D prefix. Since Wireless Client 1 and Wireless Client 2 share the same prefix (00:02:2D), traffic between the Wired Server and Wireless Clients 1 and 2 is blocked. Wireless Client 3 can still communicate with the Wired Server since it has a different prefix (00:20:A6).

Prevent All Wireless Devices From Communicating With a Single Wired Device

Configure the following settings to prevent all three Wireless Clients from communicating with Wired Server:

- **Wired MAC Address:** 00:40:F4:1C:DB:6A
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:00:00:00:00:00
- **Wireless Mask:** 00:00:00:00:00:00

Result: The unit blocks all traffic between the Wired Server and all wireless clients.

Prevent A Wireless Device From Communicating With the Wired Network

Configure the following settings to prevent Wireless Client 3 from communicating with any device on the Ethernet:

- **Wired MAC Address:** 00:00:00:00:00:00
- **Wired Mask:** 00:00:00:00:00:00
- **Wireless MAC Address:** 00:20:A6:12:4E:38
- **Wireless Mask:** FF:FF:FF:FF:FF:FF

Result: The unit blocks all traffic between Wireless Client 3 and the Ethernet network.

Prevent Messages Destined for a Specific Multicast Group from Being Forwarded to the Wireless LAN

If devices on your Ethernet network use multicast packets to communicate and these packets are not required by your wireless clients, you can set up a Static MAC filter to preserve wireless bandwidth. For example, if routers on your

network use a specific multicast address (such as 01:00:5E:00:32:4B) to exchange information, you can set up a filter to prevent these multicast packets from being forwarded to the wireless network:

- **Wired MAC Address:** 01:00:5E:00:32:4B
- **Wired Mask:** FF:FF:FF:FF:FF:FF
- **Wireless MAC Address:** 00:00:00:00:00:00
- **Wireless Mask:** 00:00:00:00:00:00

Result: The unit does not forward any packets that have a destination address of 01:00:5E:00:32:4B to the wireless network.

Static MAC Filter Configuration

Click **Configure** > **Filtering** > **Static MAC** to access the Static MAC Address filter.

Add Entries to the Static MAC Filter Table

To add the entries to Filter table, click the **Add Table Entries** button.

The following fields are may be configured or viewed:

- **Wired MAC Address:** Enter the MAC address of the device on the Ethernet network that you want to prevent from communicating with a device on the wireless network.
- **Wired Mask:** Enter the appropriate bit mask to specify the range of MAC addresses to which this filter is to apply. To specify only the single MAC address you entered in the Wired MAC Address field, enter 00:00:00:00:00:00 (all zeroes).
- **Wireless MAC Address:** Enter the MAC address of the wireless device on the wireless interface that you want to prevent from communicating with a device on the wired network.

- **Wireless Mask:** Enter the appropriate bit mask to specify the range of MAC addresses to which this filter is to apply. To specify only the single MAC address you entered in the Wireless MAC Address field, enter 00:00:00:00:00:00 (all zeroes).
- **Comment:** Enter related information.

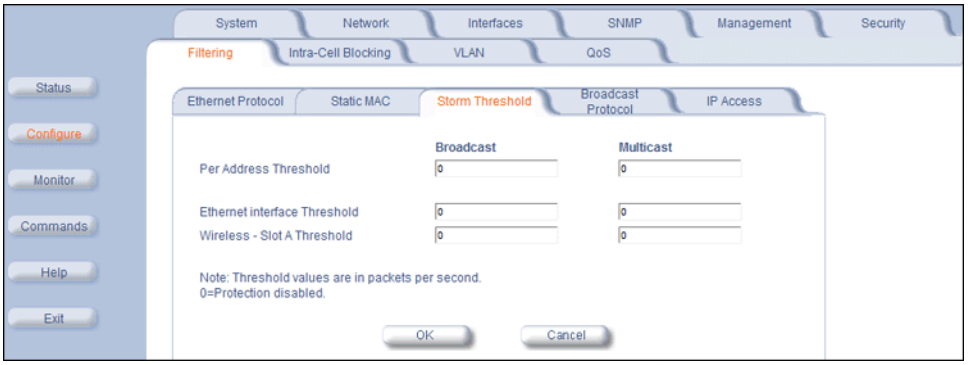
After entering the data, click the **Add** button. The entry is enabled automatically when saved.

Edit/Delete Entries in the Static MAC Filter Table

To edit an entry, click **Edit**. To disable or remove an entry, click **Edit** and change the **Status** field from **Enable** to **Disable** or **Delete**.

Storm Threshold

Click **Configure** > **Filtering** > **Storm Threshold** to use threshold limits to prevent broadcast/multicast overload.



Storm Threshold is an advanced Bridge setup option that you can use to protect the network against data overload by specifying:

- A maximum number of frames per second as received from a single network device (identified by its MAC address).
- An absolute maximum number of messages per port.

The **Storm Threshold** parameters let you specify a set of thresholds for each port of the unit, identifying separate values for the number of broadcast messages per second and multicast messages per second.

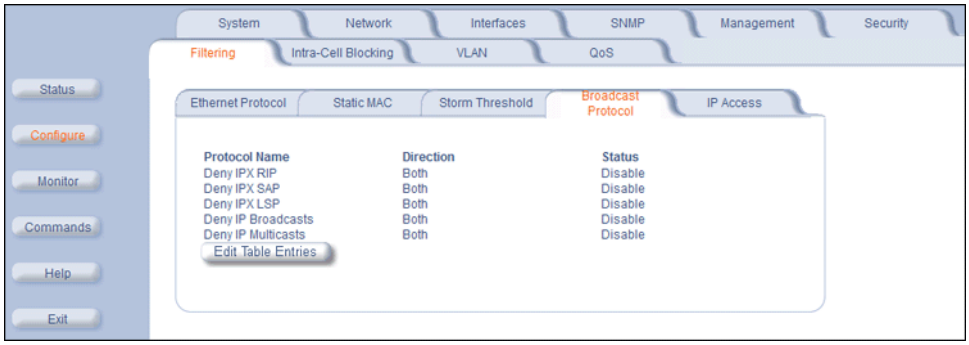
When the number of frames for a port or identified station exceeds the maximum value per second, the unit ignores all subsequent messages issued by the particular network device, or ignores all messages of that type.

The following parameters are configurable:

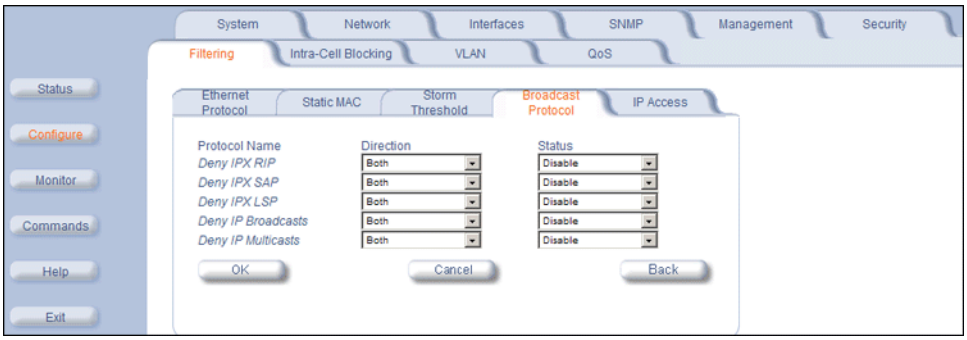
- **Per Address Threshold:** Enter the maximum allowed number of packets per second.
- **Ethernet Threshold:** Enter the maximum allowed number of packets per second.
- **Wireless Threshold:** Enter the maximum allowed number of packets per second.

Broadcast Protocol Filtering

Click **Configure** > **Filtering** > **Broadcast Protocol** to deny specific IP broadcast, IPX broadcast, and multicast traffic.



Click the **Edit Table Entries** button to display an editable window such as the following. You can configure whether this traffic must be blocked for Ethernet to wireless, wireless to Ethernet, or both.

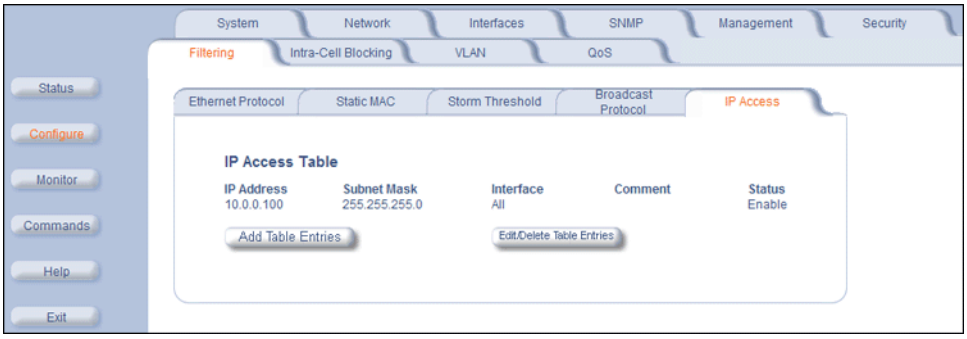


IP Access Table Filtering

Click **Configure** > **Filtering** > **IP Access Table** to limit in-band management access to the IP addresses or range of IP addresses specified in the table.

For example, **172.17.23.0/255.255.255.0** allows access from all wireless stations with an IP address in the 172.17.23.xxx range.

This feature applies to all management services (SNMP, HTTP, and CLI), except for CLI management over the serial port.

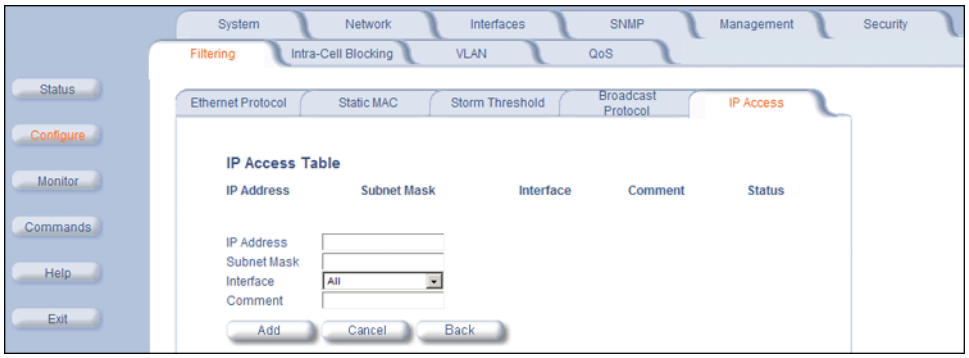


Add Entries to the IP Access Table

To add an entry, click the **Add Table Entries** button, specify the IP address and mask of the wireless stations to which you want to grant access, and click **Add**.

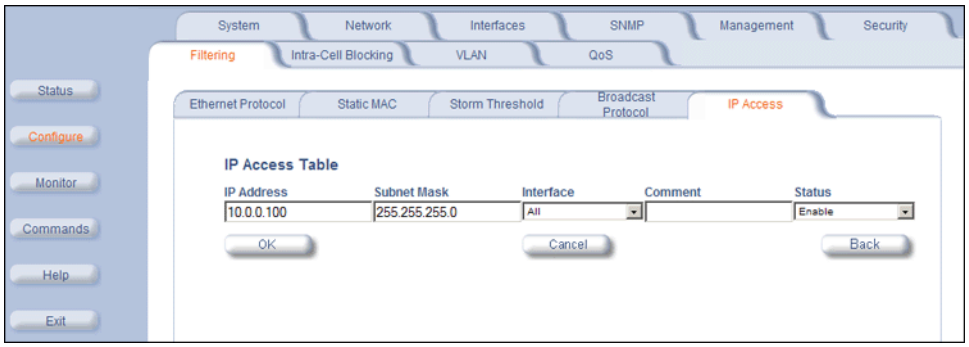
CAUTION: *Ensure that the IP address of the management PC you use to manage the unit is within the first entry in the table, as this filter takes effect immediately. Otherwise, you will have locked yourself out.*

If you do lock yourself out, you may try to give the PC the correct IP address for management; otherwise you must reset the unit via the CLI over the serial port.



Edit/Delete Entries in the IP Access Table

To edit or delete table entries, click the **Edit/Delete Table Entries** button, make your changes, and click **OK**.



Intra-Cell Blocking (BSU Only; Bridge Mode Only)

Overview

The Intra-Cell Blocking feature lets traffic be blocked between two SUs registered to the same Base Station. There are two potential reasons to isolate traffic among wireless subscribers:

- To provide better security to the subscribers by isolating the traffic from one subscriber to another in a public space.
- To block unwanted traffic between subscribers to prevent this traffic from using bandwidth.

You can form groups of SUs at the Base Station, which define the filtering criteria. All data to or from SUs belonging to the same group are bridged. All other data from SUs that do not belong to a particular group are automatically forwarded through the Ethernet interface of the Base Station. If an SU does not belong to any group, the Base Station discards the data.

You can also configure a *Security Gateway* to block traffic between SUs connected to different BSUs. All packets destined for SUs not connected to the same Base Station are forwarded to the Security Gateway MAC address (configured in the *Security Gateway* tab).

NOTE: ***Intra-Cell Blocking is configurable only in Bridge mode.*** *When you change the device from* ***Bridge*** *to* ***Routing*** *mode, Intra-Cell Blocking stops working only after a reboot. When you change the device from* ***Routing*** *to* ***Bridge*** *mode, Intra-Cell Blocking starts working only after a reboot.*

The following rules apply to Intra-Cell Blocking Groups:

- One SU can be assigned to more than one group.
- An SU that has not been assigned to any group cannot communicate to any other SU connected to the same or different BSU.

Example of Intra-Cell Blocking Groups

Assume that four Intra-Cell Blocking Groups have been configured on one BSU. SUs 1 through 6 are registered to BSU 1. SUs 7 through 9 are registered to BSU 2.

Intra-Cell Blocking Group Example			
Group 1	**Group 2**	**Group 3**	**Group 4**
SU 1	SU 2	SU 6	SU 8
SU 4	SU 3	SU 1	SU 9
SU 5	SU 8	SU 3	SU 2

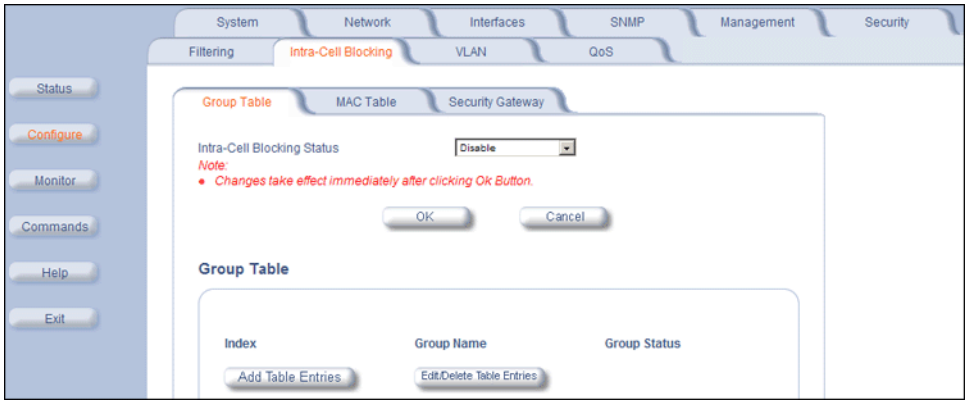
In this example, SU 1 belongs to two groups, Group 1 and Group 3. Therefore, packets from SU 1 destined to SU 4, SU 5, SU 6, and SU 3 are not blocked. However, SU 9 belongs to group 4 only and packets from SU 9 are blocked unless sent to SU 8 or SU 2.

Achieving Communication Between Two SUs

In a multipoint configuration, an SU can communicate with another SU through the BSU when in Bridge mode by default. Use the intra-cell blocking feature if this is not desired. In a routing configuration, each of the SUs must have a different subnet on their Ethernet port to distinguish traffic for each SU, and each subnet must be entered into a routing rule in the BSU as well as into an upstream router. The wireless side of all SUs must share the same subnet with the BSU wireless interface. These IP addresses must be used as next hop when creating the routes for the SU subnets.

Intra-Cell Blocking Group Table

Click **Configure** > **Intra-Cell Blocking** > **Group Table** to enable the Intra-Cell Blocking feature and to configure Intra-Cell Blocking Groups.

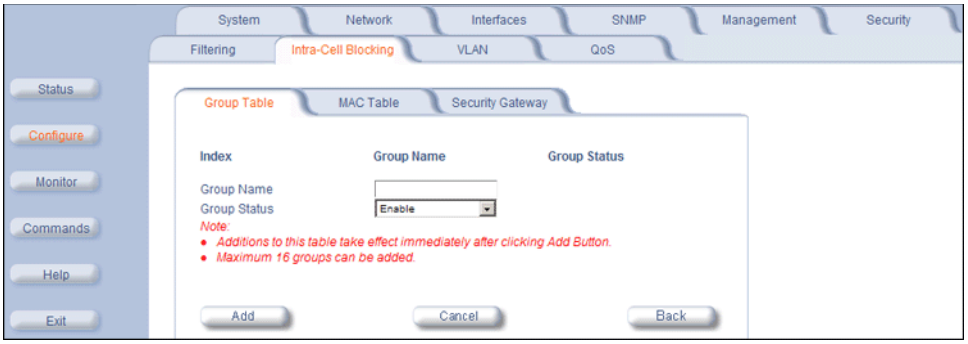


The following items are configurable:

- **Intra-Cell Blocking Status:** Enables or disables the Intra-Cell Blocking feature.
- **Group Table:** Entries in this table show the Intra-Cell Blocking filter groups that have been configured. When Intra-Cell Blocking is enabled, the Base Station Unit discards all packets coming from one SU to another SU, if both SUs do not belong to the same filter group.

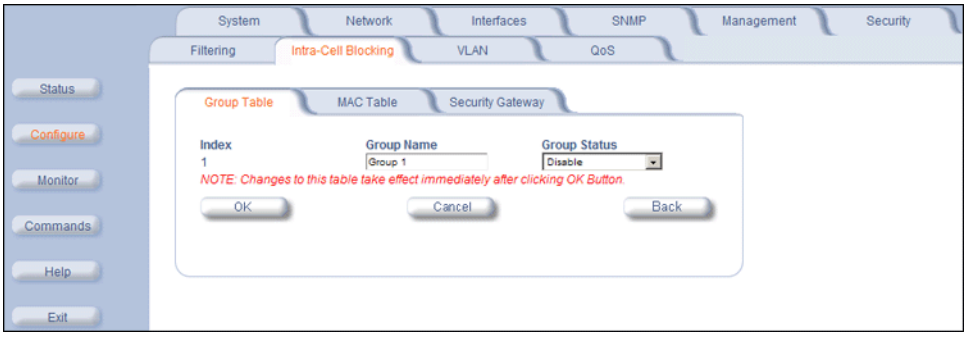
Configure Intra-Cell Blocking Groups

Click the **Add Table Entries** button to add groups to the Group Table.



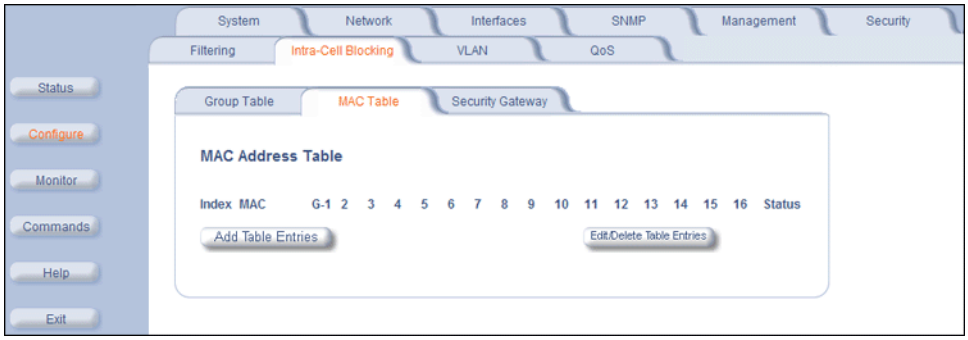
Enter the group name, and click **Add**. The group is assigned an Index and appears in the Group Table. Up to 16 groups can be configured per Base Station.

You can enable, disable or delete an existing filter group by using the **Edit/Delete Table Entries** button.



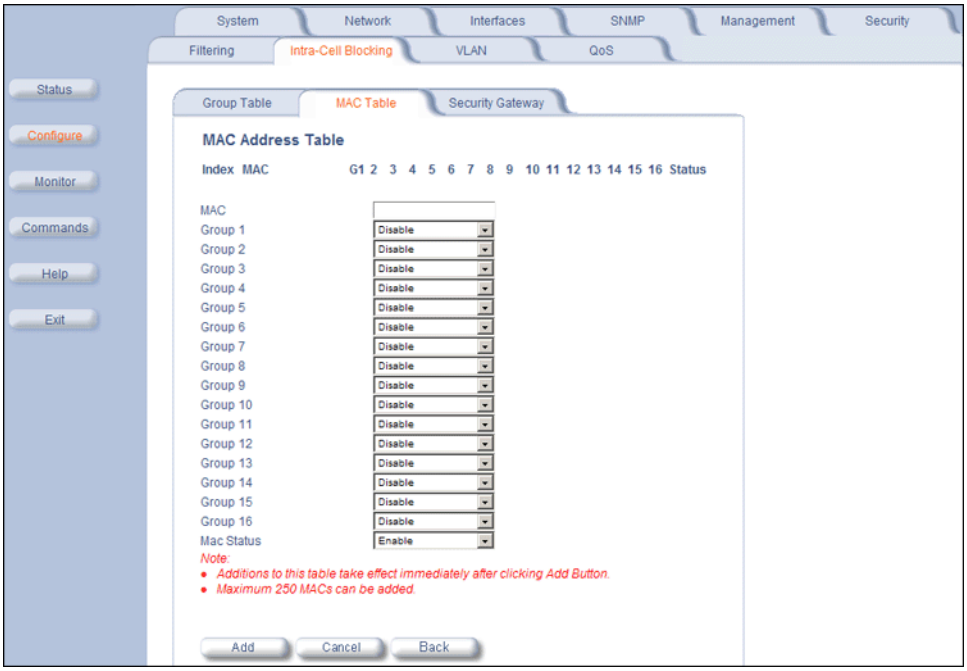
MAC Table

After configuring the Intra-Cell Blocking Groups on the **Group Table** tab, use the **MAC Table** tab to assign specific MAC addresses to an Intra-Cell Blocking Group.



Adding Entries

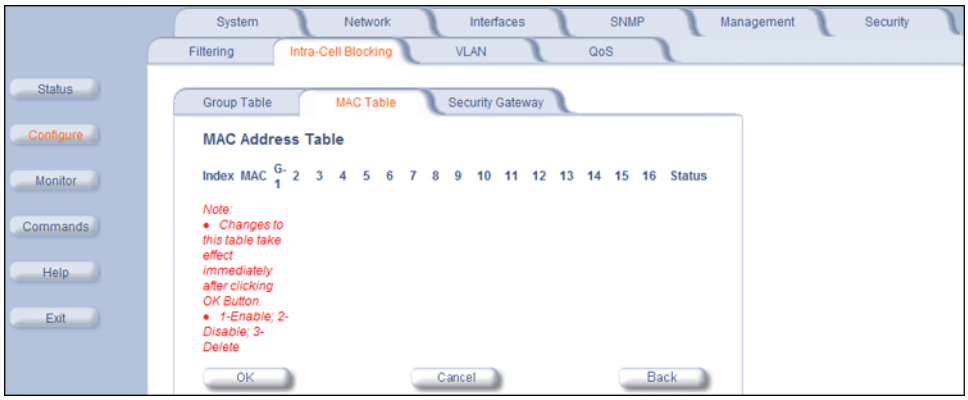
Click the **Add Table Entries** button.



Enter the MAC address of the SU. Select **Enable** from the drop-down menu for the Group Index.

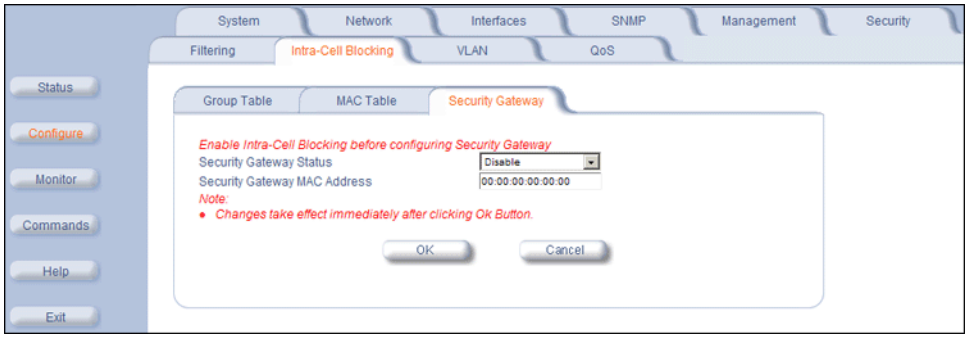
Click **Add**. The MAC address is assigned to the groups. Additions to the MAC Table take effect immediately after clicking the **Add** button.

You can **Enable**, **Disable**, **Delete**, or **Reassign** the groups for a MAC address by using the **Edit/Delete Table Entries** button. A maximum of 250 MAC addresses can be added among all filter groups.



Security Gateway

You can configure a Security Gateway to block traffic between SUs connected to different BSUs. Verify that Intra-Cell Blocking has been enabled on the **Group Table** tab before configuring the Security Gateway.



- **Security Gateway Status:** Enables or disables packet forwarding to the external Security Gateway.
- **Security Gateway MAC Address:** Lets you configure the MAC address of the external Security Gateway.

VLAN Parameters (BSU Only; Bridge Mode Only)

Overview

For an introduction to VLAN principles, see Virtual Local Area Networks (VLANs) in the System Overview chapter.

NOTE: *VLANs are configurable only in Bridge mode.*

VLAN Modes

Transparent Mode

Transparent mode is available on both the SU and the BSU. This mode is equivalent to NO VLAN support and is the default mode. It is used when the devices behind the SU and BSU are both VLAN aware and unaware. The SU/BSU transfers both tagged and untagged frames received on the Ethernet or WORP interface. Both tagged and untagged management frames can access the device.

Trunk Mode

Trunk mode is available on both the SU and the BSU. It is used when all devices behind the SU and BSU are VLAN aware. The SU and BSU transfer only tagged frames received on the Ethernet or WORP interface. Both tagged and untagged management frames can access the device.

Access Mode

Access mode is available only on the SU. It is used when the devices behind the SU are VLAN unaware. Frames to and from the Ethernet interface behind the SU map into only one VLAN segment.

Frames received on the Ethernet interface are tagged with the configured Access VLAN ID before forwarding them to the WORP interface. Both tagged and untagged management frames can access the device from the WORP interface. However, only untagged management frames can access the device from the Ethernet Interface.

Mixed Mode

Mixed mode is available on both the SU and the BSU. It is used when the devices behind the SU send both tagged and untagged data. Frames to and from the Ethernet interface behind the SU can be tagged or untagged.

Tagged frames received on the Ethernet interface are compared against the SU's trunk table, and only packets whose VLAN ID matches the trunk table are forwarded. All other packets are dropped. Untagged traffic is forwarded without any restrictions. If the BSU is in Mixed mode, the SU can be in Trunk, Access, or Mixed mode.

Q-in-Q (VLAN Stacking)

The Q-in-Q mechanism allows Service Providers to maintain customer-assigned VLANs while avoiding interference with the Service Providers' VLANs. Using the Q-in-Q mechanism, an Outer VLAN ID and Priority are added to VLAN tagged packets on top of the existing VLAN ID, such that interference is avoided and traffic is properly routed.

VLAN Forwarding

The VLAN Trunk mode provides a means to configure a list of VLAN IDs in a Trunk VLAN Table. The SU and BSU only forward frames (between Ethernet and WORP interface) tagged with the VLAN IDs configured in the Trunk VLAN Table. Up to 256 VLAN IDs can be configured for the BSU and up to 16 VLAN IDs can be configured for the SU (depending upon the capabilities of your switching equipment).

VLAN Relaying

The VLAN Trunk mode for BSU operation provides an option to enable and disable a VLAN relaying flag; when enabled, the BSU shall relay frames between SUs on the same BSU having the same VLAN ID.

Management VLAN

The BSU and SU allow the configuration of a separate VLAN ID and priority for SNMP, ICMP, Telnet, and TFTP management frames for device access.

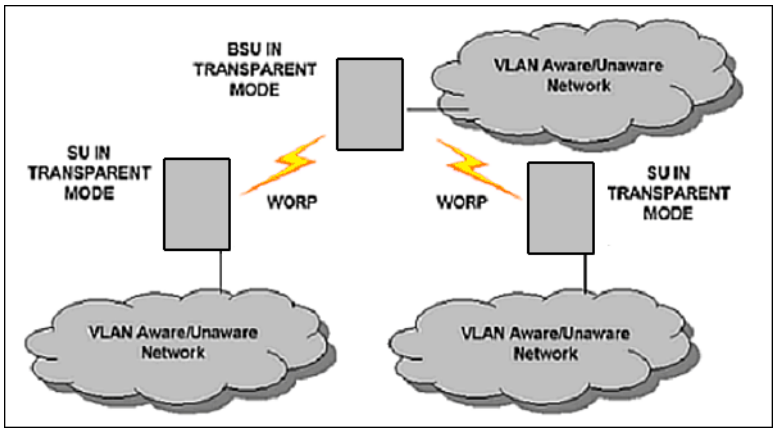
The management VLAN ID and management VLAN priority may be applied in any mode. The management stations tag the management frames they send to the BSU or SU with the management VLAN ID configured in the device. The BSU and SU tag all the management frames from the device with the configured management VLAN and priority.

BSU and SU in Transparent Mode

When the BSU is in Transparent mode, all associated SUs must be in Transparent mode.

How the BSU and SUs function in Transparent mode is described in the following table.

BSU Function – Transparent Mode	SU Function – Transparent Mode
• BSU forwards both tagged and untagged frames received from the Ethernet interface or from any of the associated SUs.	• SU forwards both tagged and untagged frames received from the Ethernet interface or from the BSU.
• If a valid management VLAN ID is configured, BSU allows only management frames tagged with the configured management VLAN ID to access it.	• If a valid management VLAN ID is configured, SU allows only management frames tagged with the configured management VLAN ID to access it.
• If a valid management VLAN ID is configured, BSU tags all management frames generated by the BSU with the configured management VLAN ID and priority.	• If a valid management VLAN ID is configured, SU tags all management frames generated by the SU with the configured management VLAN ID and priority.
• If the management VLAN ID is configured as -1 (untagged), BSU allows only untagged management frames to access it.	• If the management VLAN ID is configured as -1 (untagged), SU allows only untagged management frames to access them.

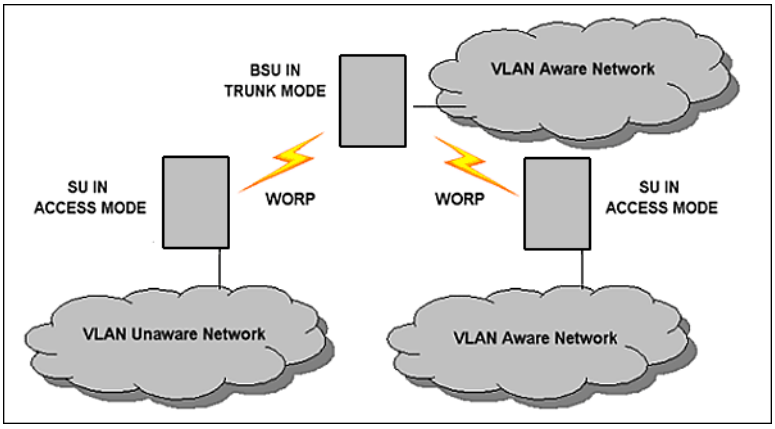


BSU in Trunk Mode and SU in Trunk/Access Mode

When the BSU is in Trunk mode, the associated SUs must be in either Trunk mode or Access mode. When an SU associates to a BSU that is in Trunk mode, it gets the VLAN mode from the BSU.

How the BSU and SU function in Trunk mode, and the SU in Access mode, is described in the following table.

BSU Function – Trunk Mode	SU Function – Trunk Mode	SU Function – Access Mode
• Up to 256 VLAN IDs can be configured on a BSU. • BSU discards all untagged frames received from the Ethernet interface or from any of the associated SUs (unexpected). • If a valid VLAN ID is configured, BSU forwards only VLAN-tagged frames received from the Ethernet interface or from any of the associated SUs that are tagged with the configured VLAN IDs; it discards all other tagged frames. • If a valid management VLAN ID is configured, BSU allows only management frames tagged with the configured management VLAN ID to access it. • If a valid management VLAN ID is configured, BSU tags all management frames generated by the BSU with the configured management VLAN ID and priority. • If the management VLAN ID is configured as -1 (untagged), BSU allows only untagged management frames to access it.	• Up to 16 VLAN IDs can be configured on an SU. • SU discards all untagged frames received from the Ethernet interface or from the BSU (unexpected). • If a valid VLAN ID is configured, SU forwards only VLAN-tagged frames received from the Ethernet interface or from the BSU that are tagged with the configured VLAN IDs; it discards all other tagged frames. • If a valid management VLAN ID is configured, SU allows only management frames tagged with the configured management VLAN ID to access it. • If a valid management VLAN ID is configured, SU tags all management frames generated by the SU with the configured management VLAN ID and priority. • If the management VLAN ID is configured as -1 (untagged), SU allows only untagged management frames to access it.	• SU discards all tagged frames received from the Ethernet interface and all untagged frames received from the BSU (unexpected). • SU tags all untagged frames received from the Ethernet interface with the configured Access VLAN ID and forwards them to the BSU. • SU untags all tagged frames received from the BSU that are tagged with the configured Access VLAN ID and forwards them to the Ethernet interface; it discards all other tagged frames from the BSU. • If a valid management VLAN ID is configured, SU allows only management frames tagged with the configured management VLAN ID to access it from the BSU. • If a valid management VLAN ID is configured, SU tags all management frames generated by the SU with the configured management VLAN ID and priority and forwards them to the BSU. • If the management VLAN ID is configured as -1 (untagged), SU allows only untagged management frames to access it from the BSU. • SU allows only untagged management frames to access it from the Ethernet interface, regardless of the value of the management VLAN ID.

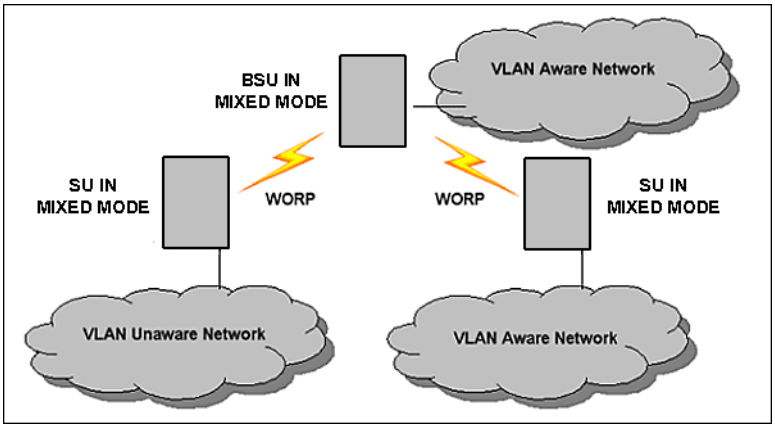


BSU in Mixed Mode and SU in Mixed, Access, or Trunk Mode

When the BSU is in Mixed mode, the associated SUs can be in Trunk, Access, or Mixed mode.

How the BSU and SU function in Trunk mode, and the SU in Access mode and Mixed mode, is described in the following table:

BSU Function – Mixed Mode	SU Function – Mixed Mode	SU Function – Trunk Mode	SU Function – Access Mode
• Up to 256 VLAN IDs can be configured on a BSU. • BSU allows all untagged frames received from the Ethernet interface or from any of the associated SUs (unexpected). • If a valid VLAN ID is configured, BSU forwards only VLAN-tagged frames received from the Ethernet interface or from any of the associated SUs that are tagged with the configured VLAN IDs; it discards all other tagged frames. • If a valid management VLAN ID is configured, BSU allows only management frames tagged with the configured management VLAN ID to access it. • If a valid management VLAN ID is configured, BSU tags all management frames generated by the BSU with the configured management VLAN ID and priority. • If the management VLAN ID is configured as -1 (untagged), BSU allows only untagged management frames to access it.	• Up to 16 VLAN IDs can be configured on an SU. • SU accepts all untagged frames received from the Ethernet interface or from the BSU (unexpected). • If a valid VLAN ID is configured, SU forwards only VLAN-tagged frames received from the Ethernet interface or from the BSU that are tagged with the configured VLAN IDs; it discards all other tagged frames. • If a valid management VLAN ID is configured, SU allows only management frames tagged with the configured management VLAN ID to access it. • If a valid management VLAN ID is configured, SU tags all management frames generated by the SU with the configured management VLAN ID and priority. • If the management VLAN ID is configured as -1 (untagged), SU allows only untagged management frames to access it.	• Up to 16 VLAN IDs can be configured on an SU. • SU discards all untagged frames received from the Ethernet interface or from the BSU (unexpected). • If a valid VLAN ID is configured, SU forwards only VLAN-tagged frames received from the Ethernet interface or from the BSU that are tagged with the configured VLAN IDs; it discards all other tagged frames. • If a valid management VLAN ID is configured, SU allows only management frames tagged with the configured management VLAN ID to access it. • If a valid management VLAN ID is configured, SU tags all management frames generated by the SU with the configured management VLAN ID and priority. • If the management VLAN ID is configured as -1 (untagged), SU allows only untagged management frames to access it.	• SU discards all tagged frames received from the Ethernet interface and all untagged frames received from the BSU (unexpected). • SU tags all untagged frames received from the Ethernet interface with the configured Access VLAN ID and forwards them to the BSU. • SU untags all tagged frames received from the BSU that are tagged with the configured Access VLAN ID and forwards them to the Ethernet interface; it discards all other tagged frames from the BSU. • If a valid management VLAN ID is configured, SU allows only management frames tagged with the configured management VLAN ID to access it from the BSU. • If a valid management VLAN ID is configured, SU tags all management frames generated by the SU with the configured management VLAN ID and priority and forwards them to the BSU. • If the management VLAN ID is configured as -1 (untagged), SU allows only untagged management frames to access it from the BSU. • SU allows only untagged management frames to access it from the Ethernet interface, regardless of the value of the management VLAN ID.



BSU VLAN Configuration

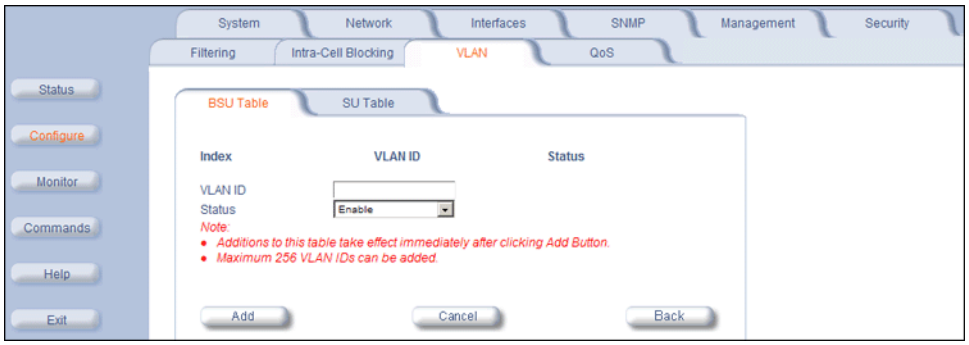
The HTTP Interface to configure BSU VLAN parameters is shown in the following figure.

Configure the following parameters:

- **BSU VLAN Mode:** The BSU VLAN mode can be either Transparent, Trunk, or Mixed. By default, the BSU is in Transparent mode.
- **Management VLAN ID:** The Management VLAN ID is configurable in any mode. The management VLAN ID has a default value of untagged and may be configured with a value in the range of 1 to 4095.
- **Management VLAN Priority:** The Management VLAN priority values range from 0 to 7 and the default priority is 0 (zero).
- **Relaying Flag:** When this flag is enabled, the BSU relays frames between SUs on the same BSU.
- **BSU VLAN Table:** The BSU VLAN Table is configurable in both Transparent and Trunk mode, but applies only when the BSU is in Trunk mode. The VLAN ID values for the BSU VLAN Table range from 1 to 4095. The maximum number of VLAN IDs that can be configured in the BSU VLAN Table is 256. An SU in Trunk mode is assigned VLAN IDs from this table.

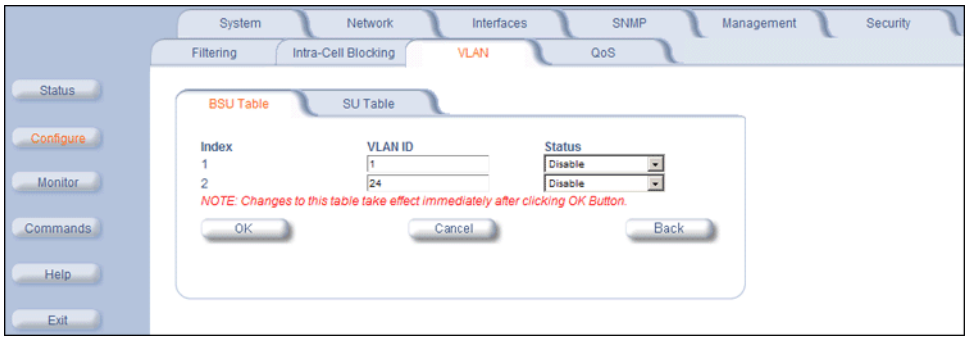
Add BSU VLAN Table Entries

To add entries to the BSU VLAN table, click the **Add Table Entries** button. Enter a **VLAN ID** and select a **Status**, then click **Add** to add your entry to the table.



Edit or Delete BSU VLAN Table Entries

To edit or delete entries in the BSU VLAN Table, click the **Edit/Delete Table Entries** button, make your changes, then click **OK** for your changes to take effect.



Restricting Unit Management

Management access to the unit can be easily secured by making management stations or hosts and the unit itself members of a common VLAN. Simply configure a non-zero management VLAN ID: management of the unit will be restricted to members of the same VLAN.

CAUTION: *If a non-zero management VLAN ID is configured, management access to the unit is restricted to hosts that are members of the same VLAN. Ensure your management platform or host is a member of the same VLAN before attempting to manage the unit or you will lose access to the unit.*

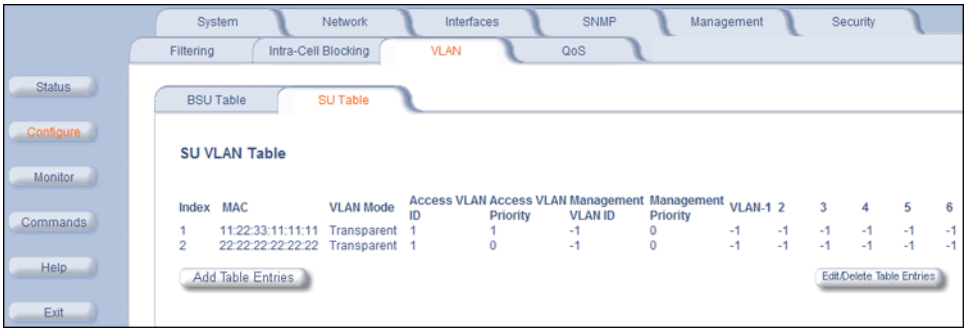
Providing Access to Hosts in the Same VLAN

The VLAN feature lets hosts manage the unit. If the **Management VLAN ID** matches a VLAN User ID, those hosts who are members of that VLAN will have management access to the unit.

CAUTION: *Once a VLAN Management ID is configured and is equivalent to one of the VLAN User IDs, all members of that VLAN will have management access to the unit. Be careful to restrict VLAN membership to those with legitimate access to the unit.*

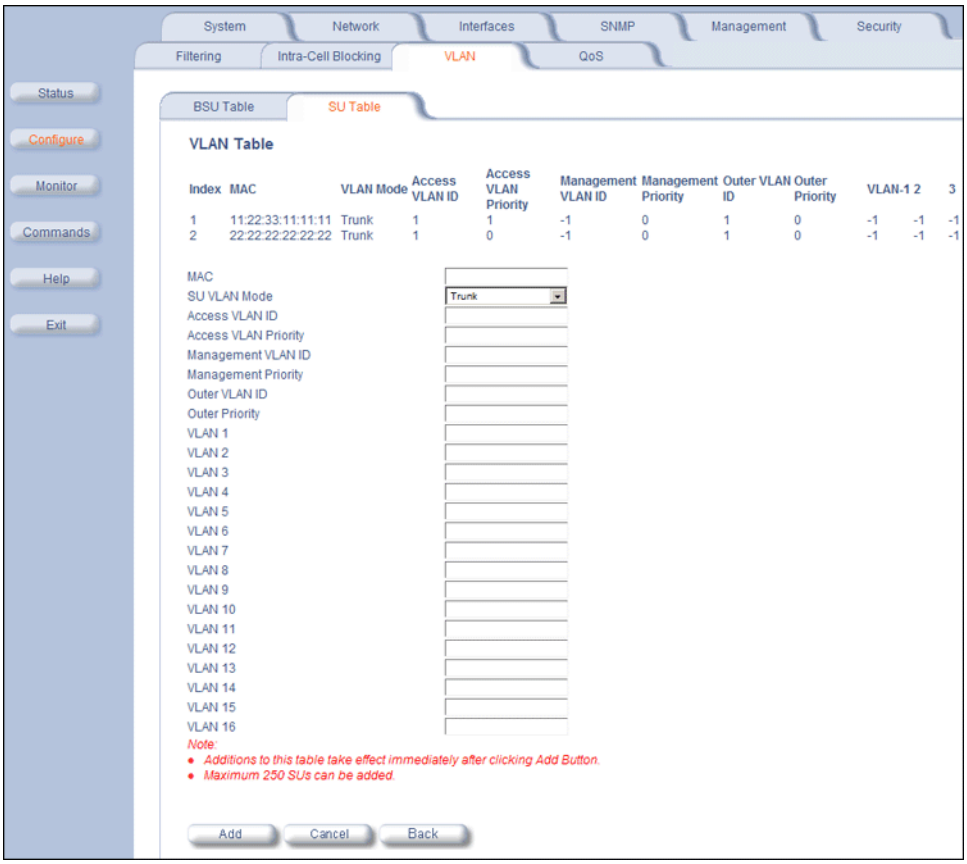
SU VLAN Configuration

The HTTP Interface to configure SU VLAN parameters is shown in the following figure.



Add SU Table Entries

To add entries to the SU VLAN Table, click the **Add Table Entries** button. Enter the desired parameters in the corresponding fields, then click **Add** to add and save the entry.



The following parameters are configurable:

- **MAC:** Enter the MAC address of the SU to be configured.
- **SU VLAN Mode:** The SU VLAN mode can be either Transparent, Trunk, Access, or Mixed (by default, the SU is in Transparent mode).
  - When the BSU is in Transparent mode, the SU must be in Transparent mode.
  - When the BSU is in Trunk mode, the SU must be in either Access mode or Trunk mode.
  - When the BSU is in Mixed mode, the SU can be in Mixed, Access, or Trunk mode.

  NOTE: *When the BSU is changed to Trunk mode, all the configured SUs are changed to Trunk mode by default.*

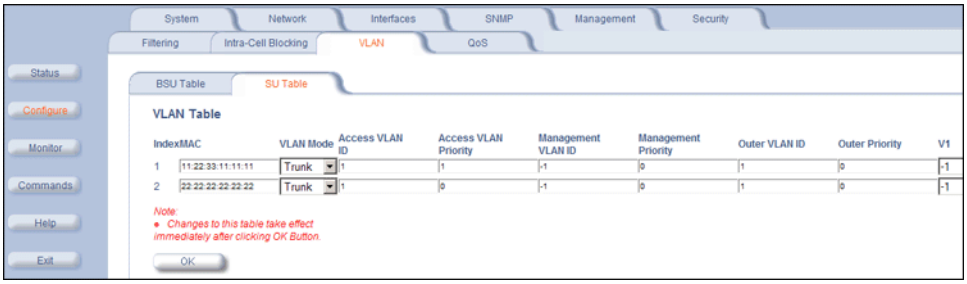
NOTE: *When the BSU is changed to Mixed mode, all the configured SUs are changed to Mixed mode by default. You may then configure SUs for Access or Trunk mode as needed.*

- **Access VLAN ID:** The Access VLAN ID is configurable in any mode, but applies only when the SU is in Access mode. The Access VLAN ID values range from 1 to 4095; the default value is 1.
- **Access VLAN Priority:** The Access VLAN Priority is configurable in any mode, but applies only when the SU is in Access mode. The Access VLAN priority values range from 0 to 7; the default priority is 0. For voice frames, the priority field is set to the VoIP configured value (5 according to latest IETF draft, or 6 according to IEEE 802.1D) regardless of the priority value configured.
- **Management VLAN ID:** The management VLAN ID is configurable in any mode. The management VLAN ID has a default value of **untagged** (-1) and may be configured with a value in the range of 1 to 4095.
- **Management Priority:** The Management VLAN priority values range from 0 to 7 and the default priority is 0 (zero).
- **Outer VLAN ID:** The Outer VLAN ID is configurable only in Trunk mode. If this parameter is set to -1, the QinQ mechanism is disabled by default. If this parameter is set to any number between 1 and 4095, all tagged data is appended with an additional VLAN ID as the outer VLAN ID.
- **Outer Priority:** The Outer VLAN Priority is configurable only in Trunk mode, and applies only when the SU is in Trunk mode and the Outer VLAN ID is configured to a value between 1 and 4095. The Outer VLAN Priority values range from 0 to 7; the default priority is 0. For voice frames, the priority field is set to the VoIP configured value, regardless of the priority value configured.
- **VLAN 1-16:** The VLAN IDs are configurable in any mode, but apply only when the SU is in Trunk mode. The VLAN ID values range from 1 to 4095; the default value is untagged (-1). The maximum number of VLAN IDs that can be configured in the SU VLAN Table is 16 for each SU. The SU VLAN IDs must be in the BSU VLAN Table that corresponds to the BSU.

Edit SU Table Entries

To edit SU table entries, click the **Edit/Delete Table Entries** button; make your changes on the window displayed, then click **OK** to save your changes.

NOTE: *If an SU is associated to a BSU, it cannot be deleted from the VLAN table.*



Typical User VLAN Configurations

VLANs segment network traffic into groups, which lets you limit broadcast and multicast traffic. These groups enable hosts from different VLANs to access different resources using the same network infrastructure. Hosts using the same physical network are limited to those resources available to their workgroup.

The unit can segment users into a maximum of 16 different VLANs per unit, based upon a VLAN ID.

The primary scenarios for using VLAN workgroups are as follows:

- **VLAN disabled:** Your network does not use VLANs.
- **VLAN enabled:** Each VLAN workgroup uses a different VLAN ID Tag. A mixture of Tagged and Untagged workgroups may be supported.

QoS (Quality of Service) Parameters (BSU Only)

The Quality of Service (QoS) feature is based on 802.16 standard and defines the classes, service flows (SFCs), and packet identification rules (PIRs) for specific types of traffic. The main priority of QoS is to guarantee a reliable and adequate transmission quality for all traffic types under conditions of high congestion and bandwidth over-subscription (for a complete discussion on QoS see Quality of Service (QoS).

For instructions on configuring a management station (a single station used for managing an entire TMP network), see QoS Configuration for a Management Station.

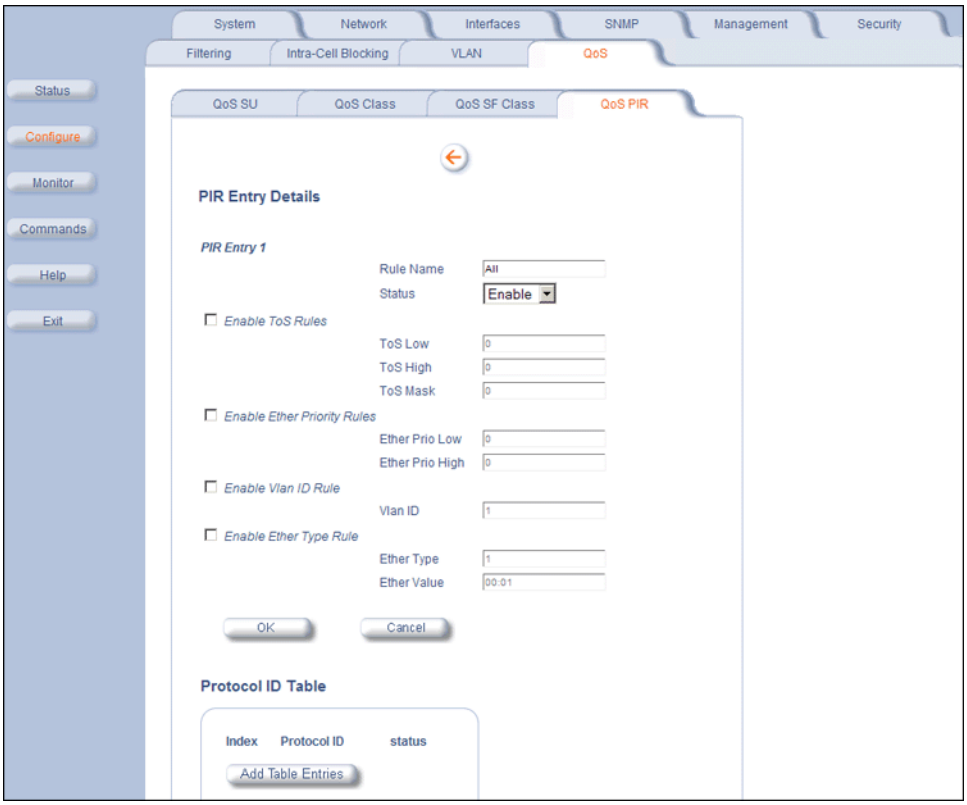
There are several pre-defined QoS classes, SFCs and PIRs available that you may choose from which cover the most common types of traffic. If you want to configure something else, build the hierarchy of a QoS class as follows:

1. Define PIRs.
2. Associate some of those PIRs to specific Service Flow classes (SFCs).
3. Assign priorities to each PIR within each SFC.
4. Define the QoS class by associating relevant SFCs to each QoS class.

QoS PIR Configuration

Click **Configure** > **QoS** > **QoS PIR Table**. The 17 predefined PIRs are shown.

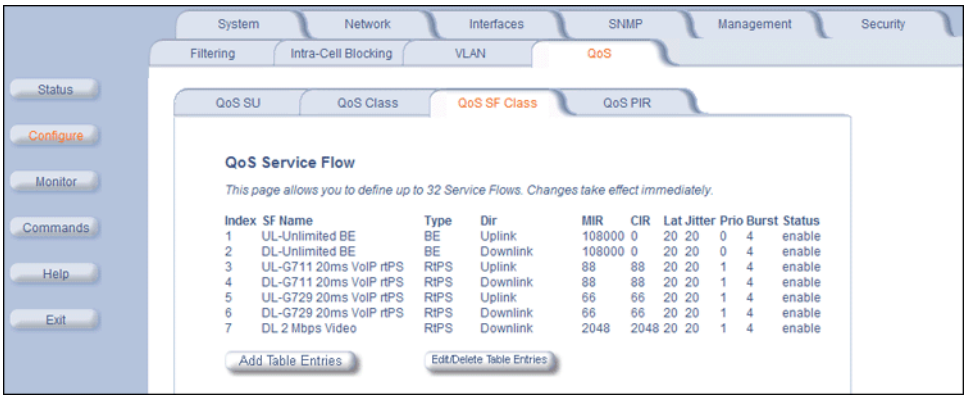
To view/edit the parameters of each PIR click on its **Details** button. You may enable, disable or delete any PIR entry by clicking on the **Status** drop-down box and then clicking **OK**.



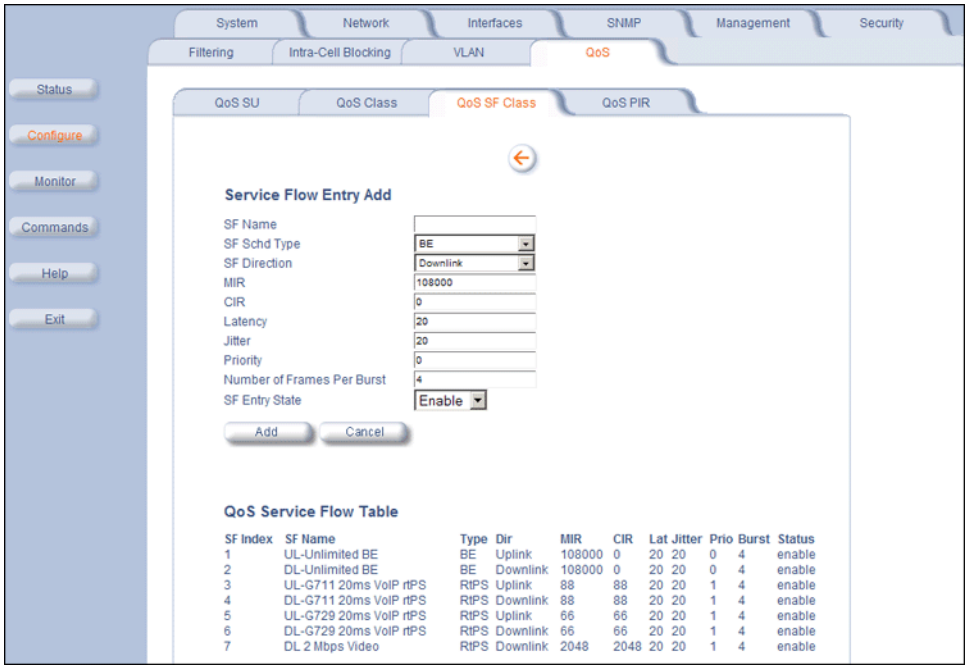
To add entries to the PIR Table, click the **Add Table Entries** button. Enter the **Rule Name** and select Enable or Disable from the **Entry Status** drop-down box, then click **Add** to add the entry. Once the new entry appears in the QoS PIR Table on this page, click its **Details** button to view/edit its parameters.

QoS SFC Configuration

Click **Configure** > **QoS** > **QoS SF Class**. The 7 predefined SFCs are shown.


System
Network
Interfaces
SNMP
Management
Security
Filtering
Intra-Cell Blocking
VLAN
QoS
Status
Configure
Monitor
Commands
Help
Exit
QoS SU
QoS Class
QoS SF Class
QoS PIR
QoS Service Flow
This page allows you to define up to 32 Service Flows. Changes take effect immediately.
Index SF Name Type Dir MIR CIR Lat Jitter Prio Burst Status
1 UL-Unlimited BE BE Uplink 108000 0 20 20 0 4 enable
2 DL-Unlimited BE BE Downlink 108000 0 20 20 0 4 enable
3 UL-G711 20ms VoIP rtPS RtPS Uplink 88 88 20 20 1 4 enable
4 DL-G711 20ms VoIP rtPS RtPS Downlink 88 88 20 20 1 4 enable
5 UL-G729 20ms VoIP rtPS RtPS Uplink 66 66 20 20 1 4 enable
6 DL-G729 20ms VoIP rtPS RtPS Downlink 66 66 20 20 1 4 enable
7 DL 2 Mbps Video RtPS Downlink 2048 2048 20 20 1 4 enable
Add Table Entries
Edit/Delete Table Entries

To add entries to the SFC Table, click the **Add Table Entries** button.



The following parameters are configurable:

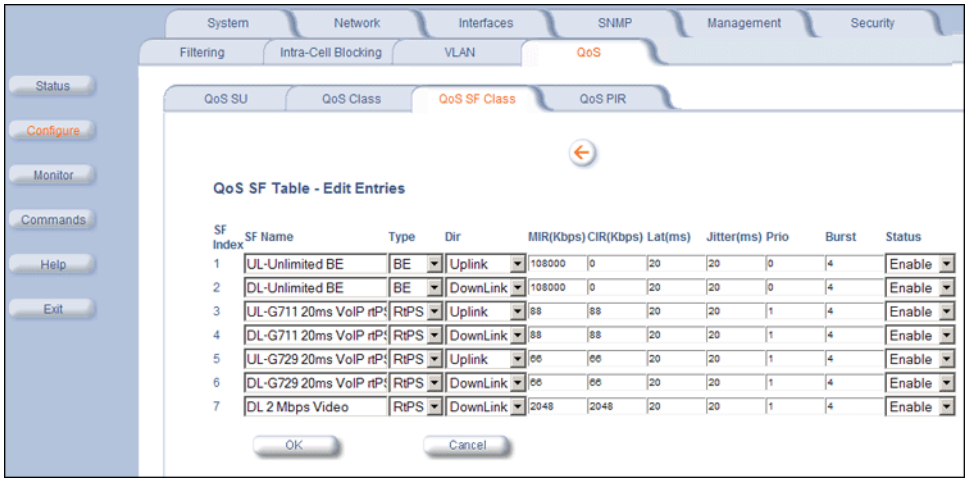
- **SF Name:** Enter the name of the SF class you want to add.
- **SF Schd Type:** This field can be set to BE (Best Effort) or RtPS (Real-Time Polling Service).
- **SF Direction:** This field can be set to Downlink (traffic from BSU to SU) or **Uplink** (traffic from SU to BSU).
- **MIR (Maximum Information Rate):** The maximum sustained data rate specified in units of 1 Kbps from 8 Kbps up to the maximum rate of 108000 Kbps per SU.
- **CIR (Committed Information Rate):** The minimum reserved traffic rate specified in units of 1 Kbps from 0 Kbps up to the maximum rate of 10000 Kbps per SU.
- **Latency:** The maximum allowed latency specified in increments of 5 ms steps from a minimum of 5 ms up to a maximum of 100 ms.
- **Jitter:** The maximum tolerable jitter specified in increments of 5 ms steps from a minimum of 0 ms up to the Maximum Latency (in ms).
- **Priority:** The priority of this SFC from zero (0) to seven (7), 0 being the lowest, 7 being the highest.
- **Number of Frames per Burst:** The maximum number of data messages in a Multi-Frame burst from one (1) to four (4), which affects the percentage of the maximum throughput of the system according to following table.

No. of messages in a burst:	% of the maximum throughput:
4	100%
3	97.6%
2	92.9%
1	76.2%

- **SF Entry State:** This field can be set to **Enable**, **Disable**, or **Delete**.

Click **Add** to add the entry. The new entry will appear on the screen, taking up the next sequential index entry.

To make changes to the entries of the SFC Table, click the **Edit/Delete Table Entries** button.

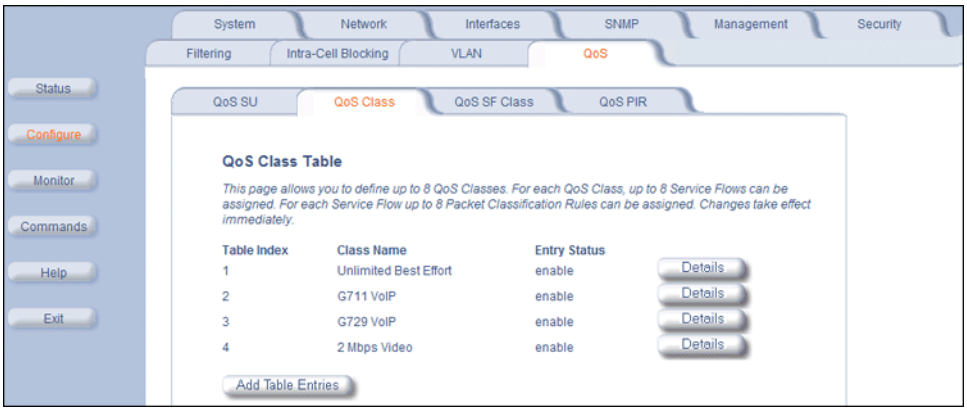


Enter your changes and click **OK**. To delete an entry, click the **Status** drop-down box and select **Delete**, then click **OK**.

QoS Class Configuration

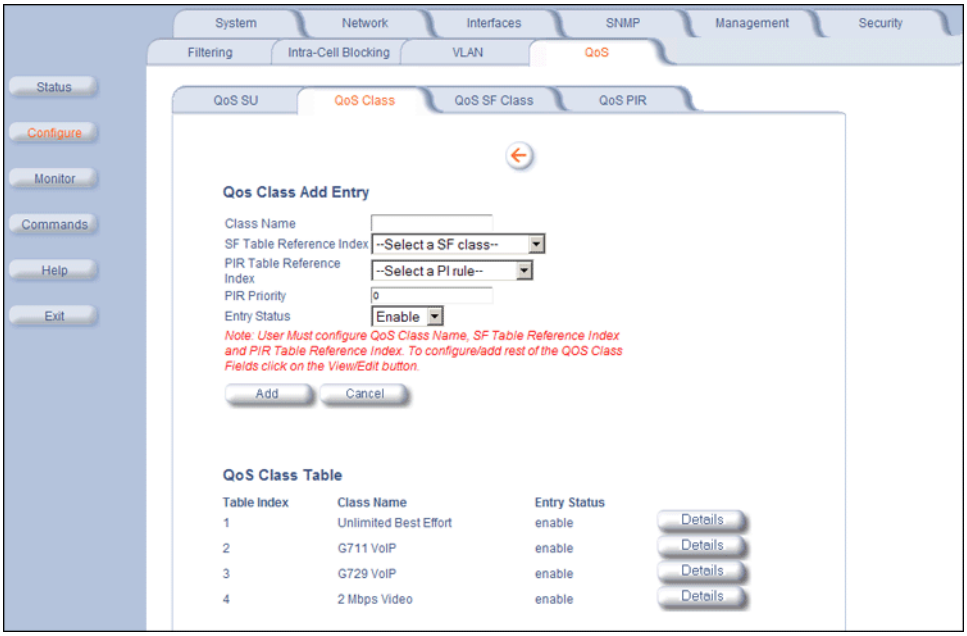
Click **Configure** > **QoS** > **QoS Class**. The 4 predefined QoS classes are shown. From this screen, you may either:

- Create a New QoS Class
- View/Edit an Existing QoS Class



Create a New QoS Class

On the QoS Class screen, click the **Add Table Entries** button.



The following parameters are configurable:

- **Class Name:** Enter the name of the QoS class you want to add.
- **SF Table Reference Index:** Select one of the possible SFCs that have been previously configured from the drop-down box to associate to this QoS Class.
- **PIR Table Reference Index:** Select one of the possible PIRs that have been previously configured from the drop-down box to associate to this SFC.
- **PIR Priority:** This priority per rule defines the order of execution of PIRs during packet identification process. The PIR priority is a number in the range 0-63, with priority 63 being executed first, and priority 0 being executed last. The PIR priority is defined within a QoS class, and can be different for the same PIR in some other QoS class. If all PIRs within one QoS class have the same priority, the order of execution of PIR rules will be defined by the order of definition of SFCs, and by the order of definition of PIRs in each SFC, within that QoS class.
- **Entry Status:** This field is always set to **Enable**.

Click **Add** to add the entry. The new entry will be listed as the next sequential index entry in the QoS Class Table.

From this screen you may also edit an existing QoS Class by clicking on its **Details** button. See View/Edit an Existing QoS Class.

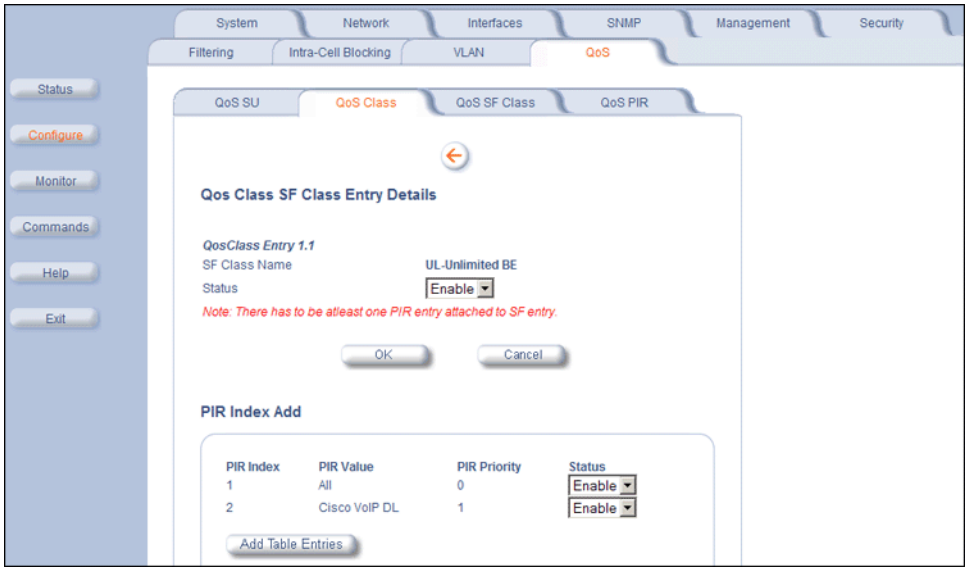
View/Edit an Existing QoS Class

To view/edit a QoS Class click on the class' **Details** button.

You may enable, disable or delete this QoS Class entry by clicking on the **Status** drop-down box and then clicking **OK**. You may also edit an existing SFC associated to this QoS class, or associate a new SFC to this QoS class. See the following sections.

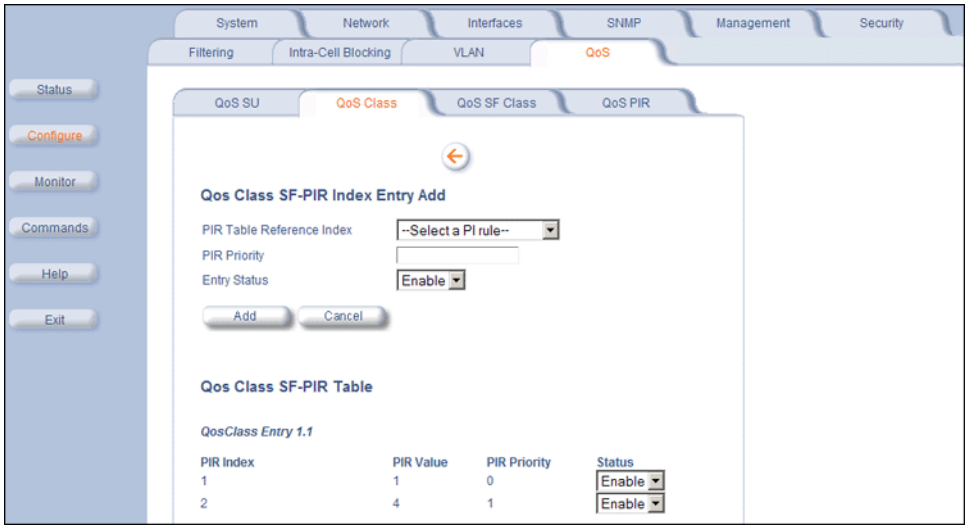
Edit an Existing SFC Associated with the QoS Class

To edit an existing SFC associated to this QoS Class, click its **Details** button.



You may enable, disable or delete this SFC entry by clicking on the **Status** drop-down box and then clicking **OK**.

To add more PIRs to this SFC click the **Add Table Entries** button.



Configure the following parameters:

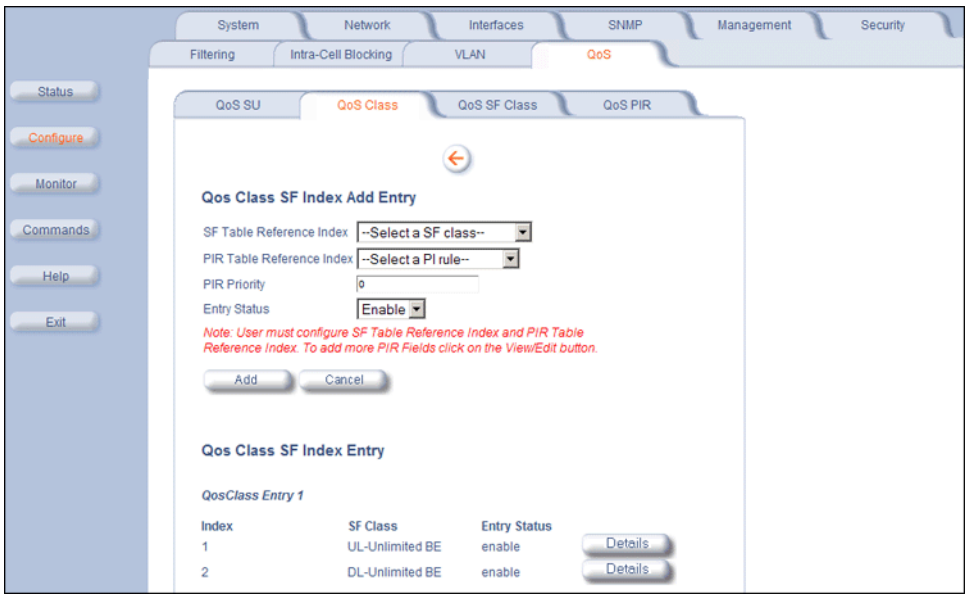
- **PIR Table Reference Index:** Select one of the possible PIRs that have been previously configured from the drop-down box.
- **PIR Priority:** This priority per rule defines the order of execution of PIRs during packet identification process. The PIR priority is a number in the range 0-63, with priority 63 being executed first, and priority 0 being executed last. The PIR priority is defined within a QoS class, and can be different for the same PIR in some other QoS class. If all PIRs within one QoS class have the same priority, the order of execution of PIR rules will be defined by the order of definition of SFCs, and by the order of definition of PIRs in each SFC, within that QoS class.
- **Entry Status:** This field is always set to **Enable**.

Click **Add** to add the entry. The new entry will be added to the PIR list, taking up the next sequential index entry.

You may delete any PIR entry by clicking on the **Status** drop-down box and selecting **Delete**.

Associate a New SFC with a QoS Class

On the QoS Class screen, click the **Details** button next to Class with which you want to associate a new SFC. Then click the **Add Table Entries** button under the **SF Details** heading to add a new SFC and associate it to this QoS Class.



The following parameters are configurable:

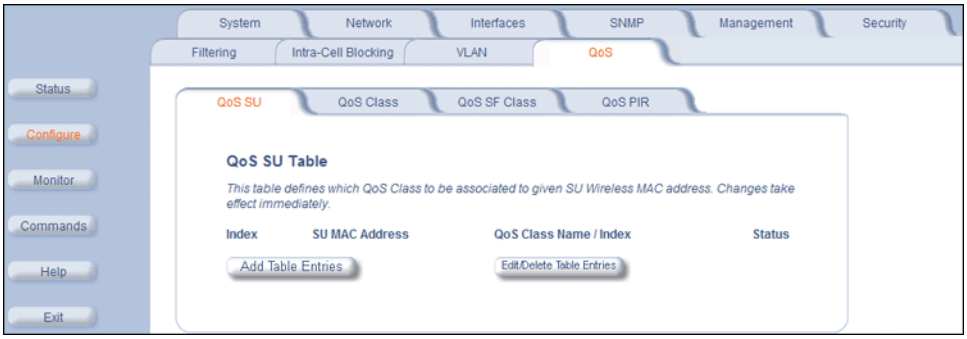
- **SF Table Reference Index:** Select one of the possible SFCs that have been previously configured from the drop-down box to associate to this QoS Class.
- **PIR Table Reference Index:** Select one of the possible PIRs that have been previously configured from the drop-down box to associate to this SFC.
- **PIR Priority:** This priority per rule defines the order of execution of PIRs during packet identification process. The PIR priority is a number in the range 0-63, with priority 63 being executed first, and priority 0 being executed last. The PIR priority is defined within a QoS class, and can be different for the same PIR in some other QoS class. If all PIRs within one QoS class have the same priority, the order of execution of PIR rules will be defined by the order of definition of SFCs, and by the order of definition of PIRs in each SFC, within that QoS class.
- **Entry Status:** This field is always set to **Enable**.

Click **Add** to add the entry. The new entry will be listed as the next sequential index entry in the SF Details table.

From this screen you may also edit an existing SFC by clicking on its **Details** button. See Edit an Existing SFC Associated with the QoS Class for more information.

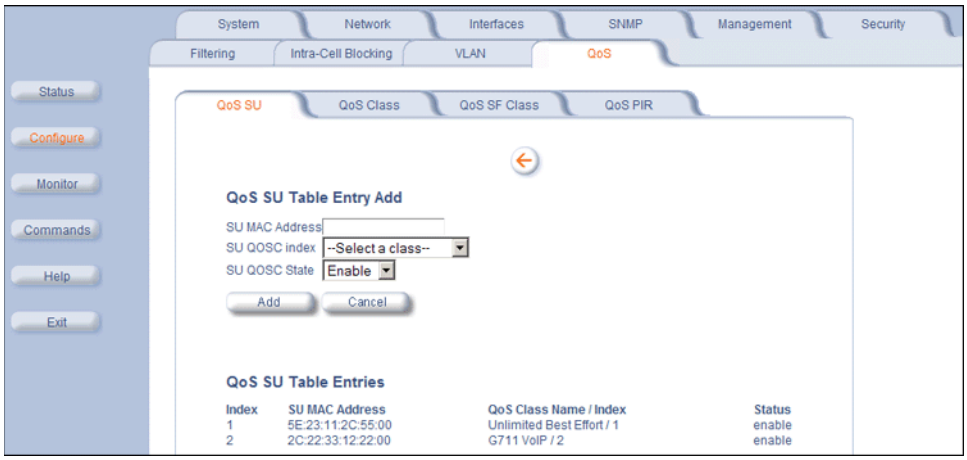
QoS SU Configuration

Click **Configure** > **QoS** > **QoS SU**.



This screen defines which QoS Classes will be associated to which SUs, using the SUs' MAC addresses.

To add entries to the QoS SU Table, click the **Add Table Entries** button.

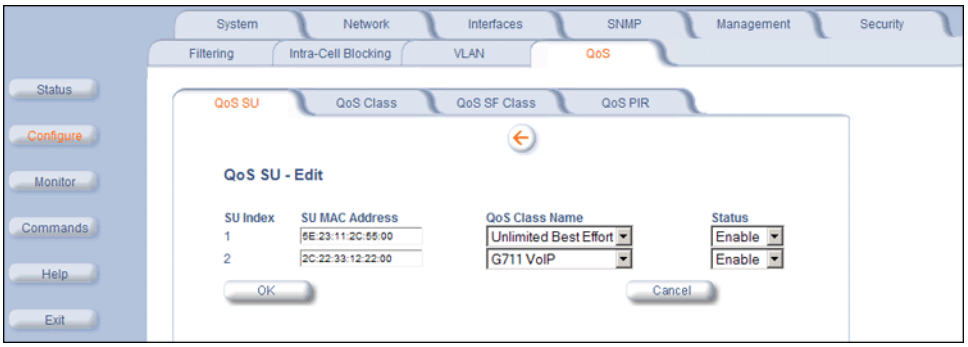


Enter the following information:

- **SU MAC Address:** The MAC Address of the SU you want to associate to a specific QoS Class.
- **SU QOSC Index:** Select one of the possible QoS Classes that have been previously configured from the drop-down box to associate to this SU.
- **SU QOSC State:** This field can be set to **Enable**, **Disable**, or **Delete**.

Click **Add** to add the entry. The new entry will be listed as the next sequential index entry in the QoS SU Table.

To make changes to the QoS SU Table, return to the QoS SU page, and click the **Edit/Delete Table Entries** button.



Enter your changes, and click **OK**. To delete an entry, click the **Status** drop-down box and select **Delete**, then click **OK**.

QoS Configuration for a Management Station

Introduction

As stated previously, the QoS feature enables prioritization of traffic and allocation of the available bandwidth based on that prioritization. The system is designed in such a way that higher priority traffic preempts lower priority traffic, keeping lower priority traffic on hold until higher priority traffic finishes. This mechanism ensures that the available bandwidth is always given first to the higher priority traffic; if all the bandwidth is not consumed, the remaining bandwidth is given to the lower priority traffic.

If QoS is not configured properly, the system can become difficult to access in heavily loaded networks. One of the side effects of this misconfiguration is ping time-out, which is usually interpreted as a disconnection of the pinged node. However, with the correct QoS configuration, every node in the network can be reached at any moment.

The configuration instructions that follow explain how to configure the system so that configuration parameters can always be changed, and ping requests and responses get higher priority in order to show the actual connectivity of the pinged node.

The configuration suggested here assumes that the whole network is managed from a single work station, called the management station. This station can be connected anywhere in the network, and can be recognized by either its IP address, or by its MAC Ethernet address if the network uses DHCP.

In this configuration, any traffic coming from or going to the management station is treated as management traffic. Therefore, the management station should be used only for configuration of the TMP.11 nodes in the network and to check connectivity of the nodes, but it should not be used for any throughput measurements.

CAUTION: *While this QoS configuration is used, the TCP or UDP throughput should not be measured from the management station.*

Step 1: Add Packet Identification Rules

To recognize management traffic, the system needs to recognize ARP requests/responses and any traffic coming from or going to the management station.

A. Confirm the Attributes of the Existing ARP PIR

The default QoS configuration contains the PIR called “ARP,” which recognizes ARP requests/responses by the protocol number 0x806 in the Ethernet Type field of the Ethernet packet. Confirm that the ARP PIR parameters are correct, as follows:

1. Click **Configure > QoS > QoS PIR**.
2. Click the **Details** button next to the ARP PIR.
3. Confirm the following attributes:
   - **Rule Name**: ARP
   - **Status**: Enable
   - **Enable Ether Type Rule**: Yes (box is checked)
     - **Ether Type**: 1
     - **Ether Value**: 08:06

B. Create New PIRs to Recognize Management Traffic

To recognize the traffic coming from or going to the management station, the system must contain two additional PIRs: one with either the destination IP address or the destination MAC address equal to the management station’s IP or MAC address, and another with either the source IP address or the source MAC address equal to the management station’s IP or MAC address.

1. Click **Configure > QoS > QoS PIR**.
2. Click **Add Table Entries**.
3. First you will configure the Destination Address PIR.
   Enter the **Rule Name:** *Management Station DST MAC Addr* if you are using a MAC addresses, or *Management Station DST IP Addr* if you are using a IP addresses.
4. Set the **Entry Status** to Enable.
5. Click **Add**. The DST Management PIR will be added to the PIR list.
6. Click the **Details** button next to the DST Management PIR you just created.
7. Scroll down to the **Destination IP Table** or the **Destination MAC Table**, depending on your configuration requirements, and click **Add Table Entries**.
8. Enter the following information:
   - **IP Address** or **MAC Address**: IP address or MAC Address of management station

- **IP Mask or MAC Mask**: 255.255.255.255 (for IP Mask) or FF:FF:FF:FF:FF:FF (for MAC mask)

9. Click **Add**.
10. Return to the **QoS PIR** tab, and click **Add Table Entries**.
11. Now you will configure the Source Address PIR. Enter the **Rule Name:**
    Enter the **Rule Name:** *Management Station SRC MAC Addr* if you are using a MAC addresses, or *Management Station SRC IP Addr* if you are using a IP addresses.
12. Set the **Entry Status** to Enable.
13. Click **Add**. The SRC Management PIR will be added to the PIR list.
14. Click the **Details** button next to the SRC Management PIR you just created.
15. Scroll down to the **Source IP Table** or the **Source MAC Table**, depending on your configuration requirements, and click **Add Table Entries**.
16. Enter the following information:
    - **IP Address** or **MAC Address**: IP address or MAC Address of management station
    - **IP Mask or MAC Mask**: 255.255.255.255 (for IP Mask) or FF:FF:FF:FF:FF:FF (for MAC mask)
17. Click **Add**.

Step 2: Add Service Flow Classes

To handle management traffic, the system needs two Service Flow Classes: one for uplink traffic, and one for downlink traffic.

A. Configure the Downlink Service Flow

1. Click **Configure > QoS > QoS SF Class**.
2. Click **Add Table Entries**.
3. Enter the following parameters:
   - **SF Name**: DL-Management
   - **SF Schd Type**: RtPS
   - **SF Direction**: Downlink
   - **MIR**: 1000
   - **CIR**: 1000
   - **Latency**: 20
   - **Jitter**: 10
   - **Priority**: 7
   - **Number of Frames Per Burst**: 4
   - **SF Entry State**: Enable
4. Click **Add**. The DL-Management SF will be added to the **QoS Service Flow Table**.

B. Configure the Uplink Service Flow

1. Remaining on the **Service Flow Entry Add** page, enter the following parameters:
   - **SF Name**: UL-Management
   - **SF Schd Type**: RtPS
   - **SF Direction**: Uplink
   - **MIR**: 1000
   - **CIR**: 1000
   - **Latency**: 20
   - **Jitter**: 10

- **Priority**: 7
- **Number of Frames Per Burst**: 4
- **SF Entry State**: Enable

2. Click **Add**. The UL-Management SF will be added to the **QoS Service Flow Table**.

NOTE: *The input and output bandwidth limits set on the BSU or on the SU are used for limiting aggregate bandwidth used by singe SU. These limits override any limit imposed by MIR in the SFC; thus, these limits should be set to at least 1000 kbps (MIR values in UL-Management and DL-Management SFCs).*

Step 3: Configure QoS Classes

Finally, the DL-Management SFC and UL-Management SFCs created in Step 2 must be added to each QoS Class used by the TMP.11 network. Additionally, within the QoS class, these SFC must have the three PIRs mentioned in Step 1 associated with them.

A. Add SFCs to QoS Class

1. Click **Configure > QoS > QoS Class**.
2. Click the **Details** button next to the first class you wish to modify.
3. Under the **SF Details** heading, click **Add Table Entries**.
4. Configure the following parameters:
   - **SF Table Reference Index**: DL-Management
   - **PIR Table Reference Index**: ARP
   - **PIR Priority**: 63
   - **Entry Status**: Enable
5. Click **Add**. The DL-Management SF will be added to the **Qos Class SF Index Entry** list at the bottom of the page.
6. Remaining on this page, configure the parameters for the other UL-Management SF:
   - **SF Table Reference Index**: UL-Management
   - **PIR Table Reference Index**: ARP
   - **PIR Priority**: 63
   - **Entry Status**: Enable
7. Click **Add**. The UL-Management SF will be added to the **Qos Class SF Index Entry** list at the bottom of the page.
8. Return to the **QoS Class** screen, and repeat steps 1- 7 for any other QoS classes used in the network.

B. Add PIRs to SFCs within the QoS Class

1. Click **Configure > QoS > QoS Class**.
2. Click the **Details** button next to the first class you wish to modify.
3. Under the **SF Details** heading, click the **Details** button next to the DL-Management SF.
4. Under the **PIR Index Add** heading, click the **Add Table Entries** button.
5. Add the *DST Management* (whether IP or MAC) PIR to this SF by configuring the following parameters:
   - **PIR Table Reference Index**: Management Station DST MAC Addr or Management Station DST IP Addr
   - **PIR Priority**: 63
   - **Entry Status**: Enable
6. Click **Add**. The PIR will be added to the **Qos Class SF-PIR** list at the bottom of the page.
7. Remaining on this page, add the SRC Management PIR to this SF by configuring the following parameters:
   - **PIR Table Reference Index**: Management Station SRC MAC Addr or Management Station SRC IP Addr
   - **PIR Priority**: 63

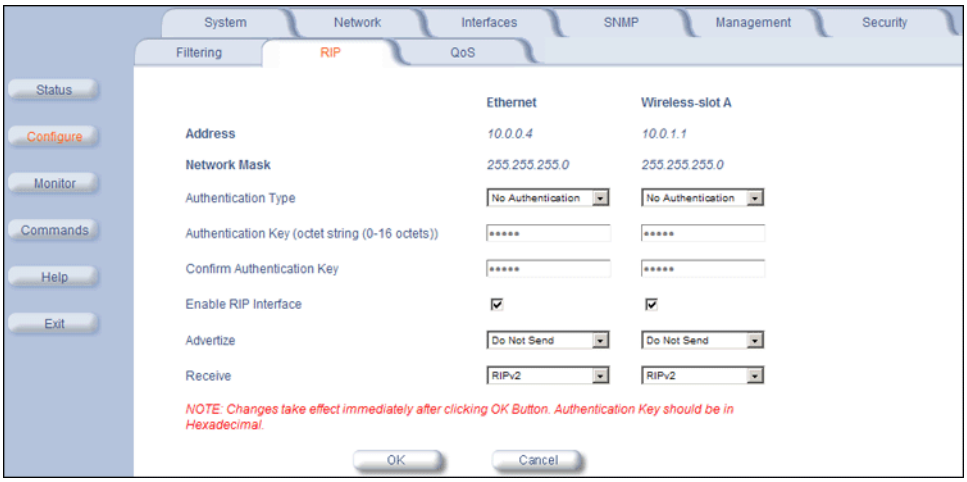
- **Entry Status**: Enable

8. Return to the **QoS Class** screen and repeat steps 2 - 6 for the UL-Management SF in this class.
9. Return to the **QoS Class** screen and repeat steps 1 - 8 for any other QoS Classes used in the network.

RIP Parameters (Routing Mode Only)

Routing Internet Protocol (RIP) is a dynamic routing protocol you can use to help automatically propagate routing table information between routers. The unit can be configured as RIPv1, RIPv2, RIPv1 Compatible, or a combination of the three versions while operating in **Routing** mode. In general, the unit's RIP module is based upon RFC 1389.

NOTE: *RIP is configurable only when the unit is in Routing Mode and Network Address Translation (NAT) is disabled.*



Note the following:

- RIPv2 is enabled by default when routing mode is selected.
- You may turn RIP off by clearing the Enable RIP Interface check box for the Ethernet or the wireless interface. Any RIP advertisements that are received on the designated interface are ignored. All other options on the page are dimmed.
- If the Enable RIP Interface check box is selected, the unit sends RIP requests and "listens" for RIP updates coming from RIP-enabled devices advertising on the network. You may configure the Receive field for RIPv1, RIPv2, or a combination of both. Although the unit receives and processes these updates, it does not further propagate these updates unless configured to advertise RIP. Again, you may configure the **Advertize** field for RIPv1, RIPv2, or a combination of both.
- The ability to enable or disable default route propagation is not user configurable. Once initialized, the unit uses its static default route and does not advertise this route in RIP updates. If another router on your network is configured to advertise its default route, this route overwrites the static default route configured on the unit. The unit then also propagates the new dynamic default route throughout the network.

Be aware that, once a dynamic default route is learned, it behaves just as any other dynamic route learned through RIP. This means if the device sending the default route stops sending RIP updates, the default route times out and the unit has no default route to the network. Workarounds for this condition include rebooting or re-entering a static default route. In general, the best approach is to disable the propagation of default routes on the other routers in your network unless you understand the risks.

The following table describes the properties and features of each version of RIP supported.

RIPv1	RIPv2	RIPv1 Compatible
Broadcast	Multicast	Broadcast
No Authentication	Authentication	Authentication
Class routing	Classless routing (VLSM)	Classless routing (VLSM)
Distance-vector protocol	Distance-vector protocol	Distance-vector protocol
Metric-Hops	Metric-Hops	Metric-Hops

RIPv1	RIPv2	RIPv1 Compatible
Maximum Distance 15	Maximum Distance 15	Maximum Distance 15
IGP	IGP	IGP

RIP Example

In the following example, assume that both the BSU and the SUs all are configured in **Routing** mode with RIP enabled to send and receive on both the Ethernet and Wireless interfaces. The network converges through updates until each unit has the following routing table:

BSU

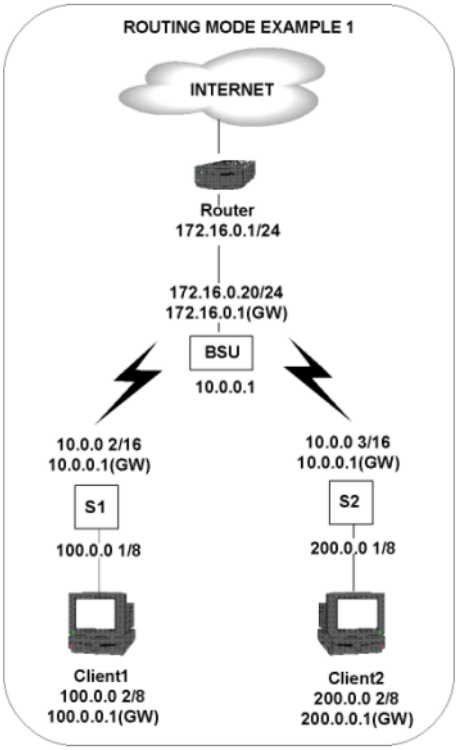
```
0.0.0.0         172.16.0.1     metric 1
172.16.0.0      172.16.0.20    metric 1
10.0.0.0        10.0.0.1       metric 1
100.0.0.0       10.0.0.2       metric 2
200.0.0.0       10.0.0.3       metric 2
```

SU1

```
0.0.0.0         10.0.0.1       metric 1
10.0.0.0        10.0.0.2       metric 1
100.0.0.0       100.0.0.1      metric 1
172.16.0.0      10.0.0.1       metric 2
200.0.0.0       10.0.0.2       metric 2
```

SU2

```
0.0.0.0         10.0.0.1       metric 1
10.0.0.0        10.0.0.3       metric 1
200.0.0.0       200.0.0.1      metric 1
172.16.0.0      10.0.0.1       metric 2
100.0.0.0       10.0.0.2       metric 2
```



RIP Notes

- Ensure that routers on the same physical network are configured to use the same version of RIP.
- Routing updates occur every 30 seconds. It may take up to 3 minutes for a route that has gone down to timeout in a routing table.
- RIP is limited to networks with 15 or fewer hops.

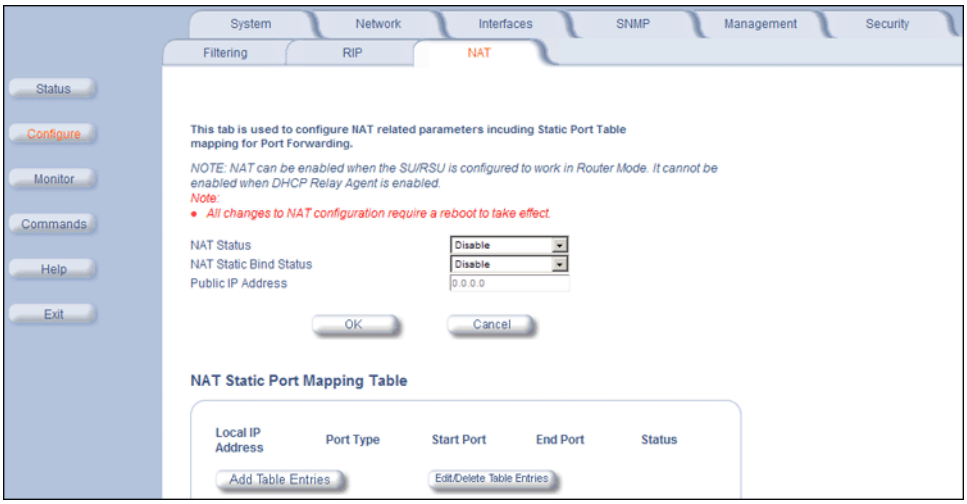
NAT (SU Only; Routing Mode Only)

The NAT (Network Address Translation) feature lets hosts on the Ethernet side of the SU transparently access the public network through the BSU. All hosts in the private network can have simultaneous access to the public network.

NOTE: ***The NAT tab is available for SUs in Routing mode only.*** *The SU supports NAPT (Network Address Port Translation) where all private IP addresses are mapped to a single public IP address, and does not support Basic NAT (where private IP addresses are mapped to a pool of public IP addresses).*

Both **dynamic mapping** (allowing private hosts to access hosts in the public network) and **static mapping** (allowing public hosts to access hosts in the private network) are supported:

- In dynamic mapping, the SU maps the private IP addresses and its transport identifiers to transport identifiers of a single Public IP address as they originate sessions to the public network. This is used only for outbound access.
- Static mapping is used to provide inbound access. The SU maps a private IP address and its local port to a fixed public port of the global IP address. This is used to provide inbound access to a local server for hosts in the public network. Static port mapping allows only one server of a particular type. Up to 1000 ports (500 UDP and 500 TCP) are supported.



The following parameters are configurable:

NOTE: *Changes to NAT parameters, including the NAT Static Port Mapping Table, require a reboot to take effect.*

NOTE: *When NAT is enabled, the DHCP Relay Agent feature is not supported (DHCP Relay Agent must be disabled before NAT is enabled) and RIP updates are not sent or received. You can configure a DHCP server to allocate IP addresses to hosts on the Ethernet side of the SU/ BSU (see* DHCP Server*).*

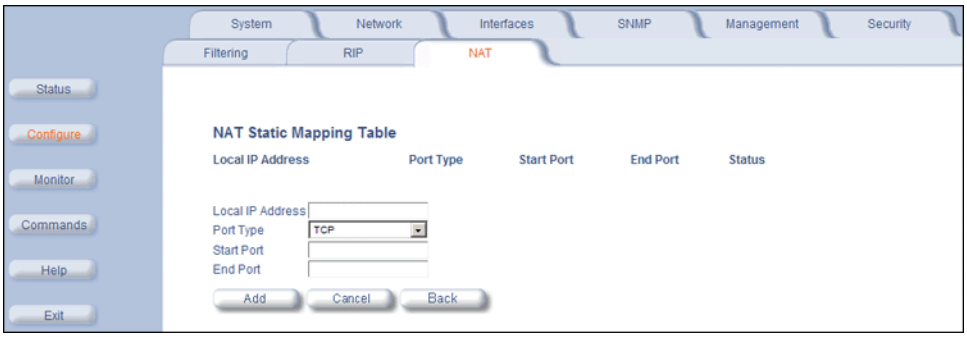
- **NAT Status:** Enables or disables the NAT feature. NAT can be enabled only for SUs in Routing mode. The default is disabled.
- **NAT Static Bind Status:** Enables or disables the NAT Static Bind status (static mapping) allowing public hosts to access hosts in a private network. The default is disabled.
- **Public IP Address:** The NAT Public IP address is the wireless interface IP address.

NAT Static Port Mapping Table

Adding entries to the NAT Static Mapping Table lets configured hosts in a private address realm on the Ethernet side of the SU access hosts in the public network using Network Address Port Translation (NAPT). Up to 1000 entries can be configured (500 UDP ports and 500 TCP ports).

Add Entries to the NAT Static Port Mapping Table

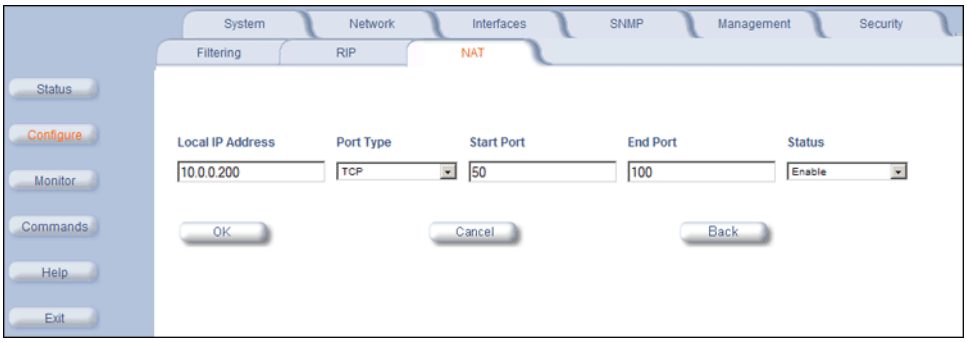
1. Click the **Add Table Entries** button.



2. Enter the following information, and click **Add**:
   - Enter the **Local IP Address** of the host on the Ethernet side of the SU.
   - Select the **Port Type**: **TCP**, **UDP**, or **Both**.
   - Enter the **Start Port** and **End Port**.

Edit/Delete Entries in the NAT Static Port Mapping Table

1. Click the **Edit/Delete Table Entries** button.



2. Enter your changes. To delete an entry, click the **Status** drop-down box and select **Delete**. Then Click **OK**.

Supported Session Protocols

The NAT feature supports the following session protocols for both inbound and outbound access with the required support, applications, and limitations given in the following table.

Certain Internet applications require an Application Level Gateway (ALG) to provide the required transparency for an application running on a host in a private network to connect to its counterpart running on a host in the public network. An ALG may interact with NAT to set up state information, use NAT state information, modify application specific payload and perform the tasks necessary to get the application running across address realms.

No more than one server of a particular type is supported within the private network behind the SU.

These VPN protocols are supported with their corresponding ALGs: IPsec, PPTP, L2TP.

The following session protocols are supported:

Protocol	Support	Applications	Limitations
ICMP	ICMP ALG	Ping	
FTP	FTP ALG	File transfer	

Protocol	Support	Applications	Limitations
H.323	H.323 ALG	Multimedia conferencing	
HTTP	Port mapping for inbound connection.	Web browser	
TFTP	Port mapping for inbound connection.	File transfer	
Telnet	Port mapping for inbound connection.	Remote login	
CUSeeMe	Port mapping for inbound and outbound connection.	Video conferencing	One user is allowed for video conferencing
IMAP	Port mapping for inbound connection.	Mail	
PNM	Port mapping for inbound connection.	Streaming media with Real Player	
POP3	Port mapping for inbound connection.	E-mail	
SMTP	Port mapping for inbound connection.	E-mail	Mails with IP addresses of MTAs or using IP addresses in place of FQDN are not supported (requires SMTP ALG).
RTSP	Port mapping for inbound connection.	Streaming audio/video with Quick Time and Real Player	
ICQ	Port mapping for inbound connection.	Chat and file transfer	Each host using ICQ needs to be mapped for different ports.
IRC	Port mapping for inbound connection.	Chat and file transfer	Each host using IRC needs to be mapped for different ports.
MSN Messenger	Port mapping for inbound and outbound connection.	Conference and Share files with Net meeting	Only one user is allowed for net meeting.
Net2Phone	Port mapping for inbound and outbound connection.	Voice communication	
IP Multicast	Pass Through	Multicasting	
Stream works	Port mapping for inbound connection.	Streaming video	
Quake	Port mapping for inbound connection.	Games	When a Quake server is configured within the private network behind a SU, the SU cannot provide information about that server on the public network. Also, certain Quake servers do not let multiple users log in using the same IP address, in which case only one Quake user is allowed.

7 Monitoring

This chapter describes using the Web interface to obtain detailed information about the settings and performance of the unit.

Click the **Monitor** button to access this information.

The following tabs appear in the **Monitor** section:

- Wireless
- ICMP
- Per Station
- Features
- Link Test
- Interfaces
- IP ARP Table
- IP Routes
- Learn Table
- RIP
- RADIUS (BSU Only)
- QoS (BSU Only)

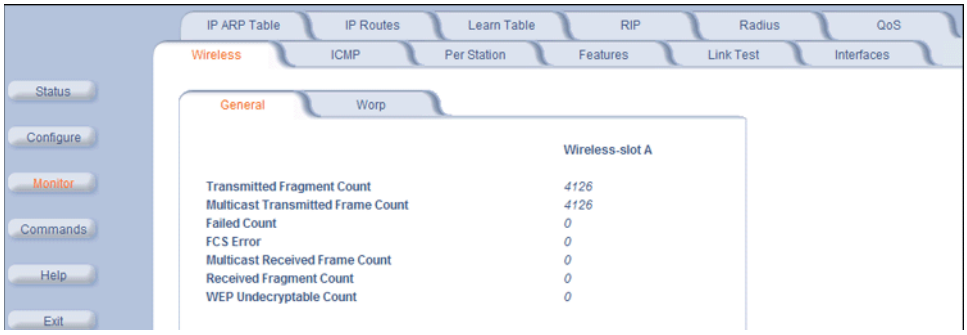
Help and Exit buttons also appear on each page of the Web interface; click the **Help** button to access online help; click the **Exit** button to exit the application.

For an introduction to the basics of management, see Basic Management.

Wireless

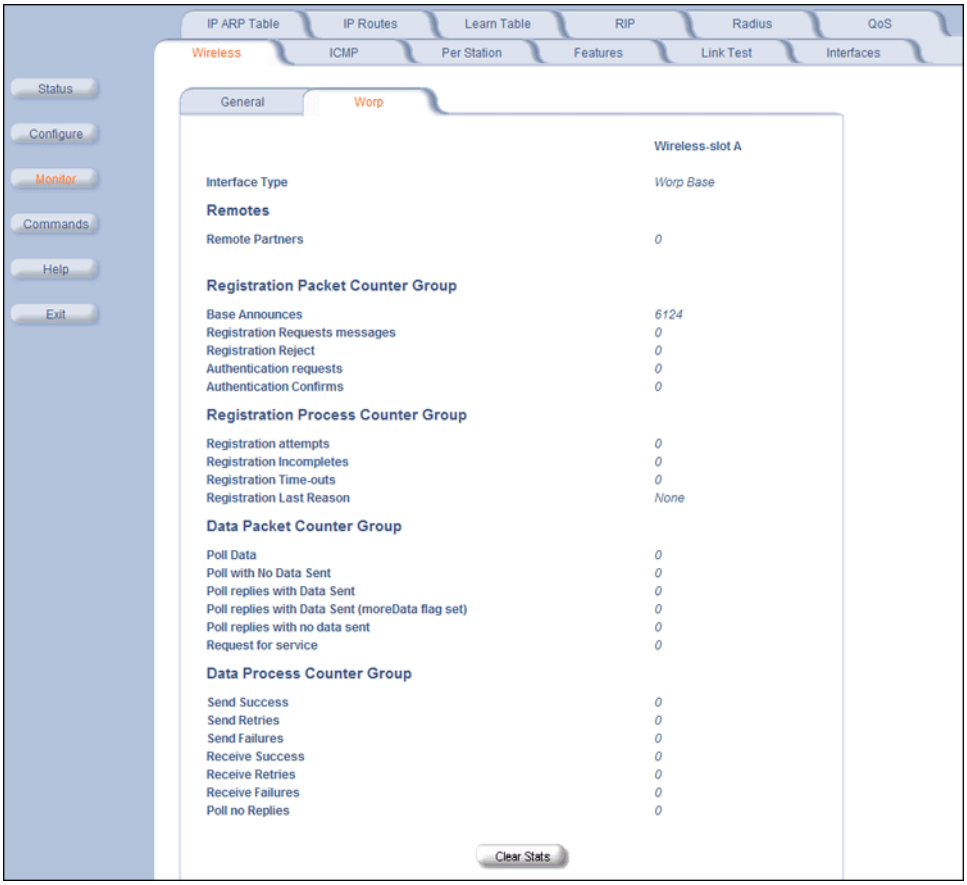
General Performance

Click **Monitor** > **Wireless** > **General** to monitor the general performance of the wireless interface.



WORP Interface Performance

Click **Monitor** > **Wireless** > **WORP** tab to monitor the performance of the WORP Base or WORP SU interfaces.



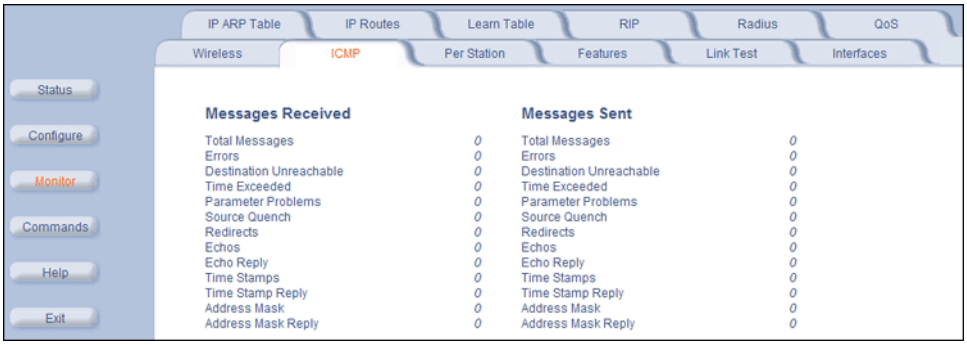
The **Registration Last Reason** field indicates either a successful registration (a value of 1) or it indicates the reason why the last registration failed. Possible values for the **Registration Last Reason** field are as follows:

- None (successful registration)
- Maximum number of SUs reached

- Authentication failure
- Roaming
- No response from SU within the Registration Timeout Period
- Low Signal Quality

ICMP

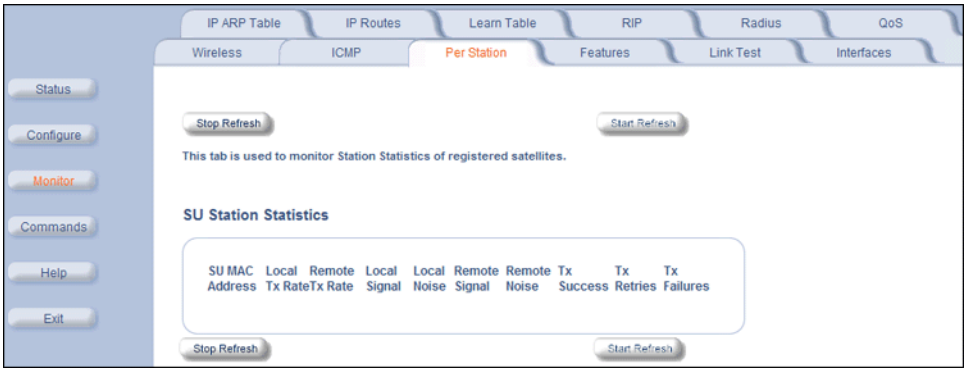
Click **Monitor** > **ICMP** to view the number of ICMP messages sent and received by the unit. It includes **ping**, **route**, and **host unreachable** messages.



Per Station

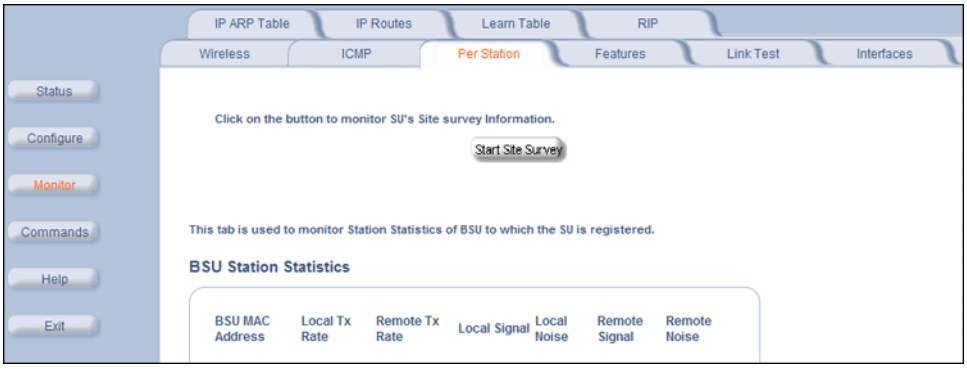
Click **Monitor** > **Per Station** to view Station Statistics. On the BSU, this page shows statistics of all the SU's connected to the BSU.

The page's statistics refresh every 4 seconds. To stop or stop the page refreshing, use the **Stop Refresh** and **Start Refresh** buttons.



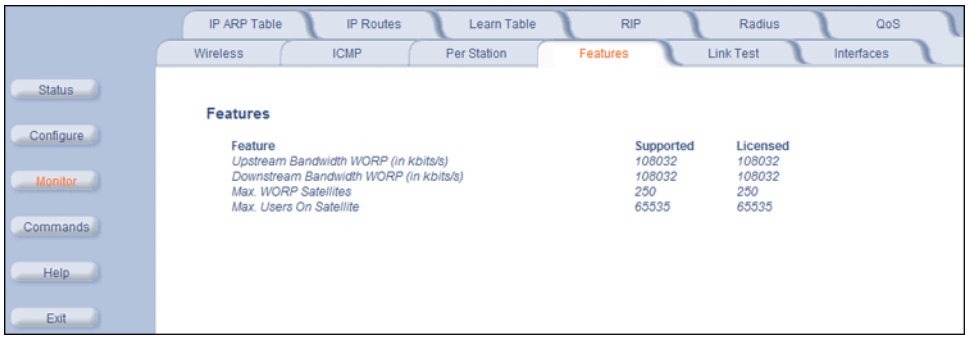
Site Survey

The SU Per Station page contains a Site Survey function. When Site Survey is activated, the SU scans all the available channels and channel bandwidths, and collects information about all the BSUs on those channels/bandwidths. The SU page is shown below.



Features

Click **Monitor** > **Features** to view the following information.



NOTE: *A BSU shows how many WORP SUs it can support; the SU shows how many Ethernet hosts it supports on its Ethernet port as the "Max Users on Satellite" parameter.*

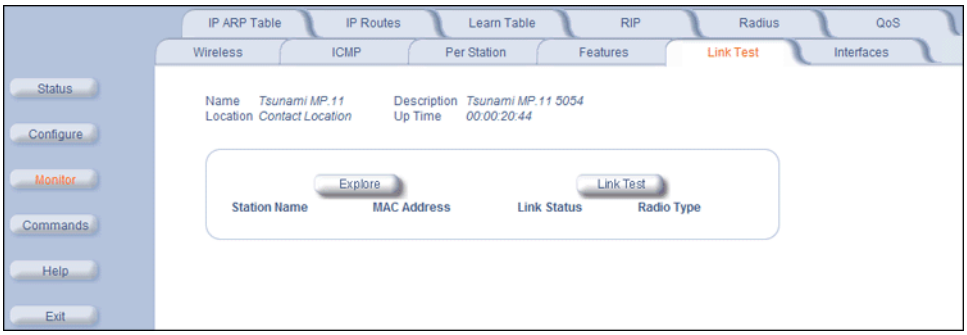
Link Test

Click **Monitor** > **Link Test** to find out which wireless stations are in range and to check their link quality.

NOTE: *Link Test requires Internet Explorer version 6.0 or later. Earlier versions do not support Link Test.*

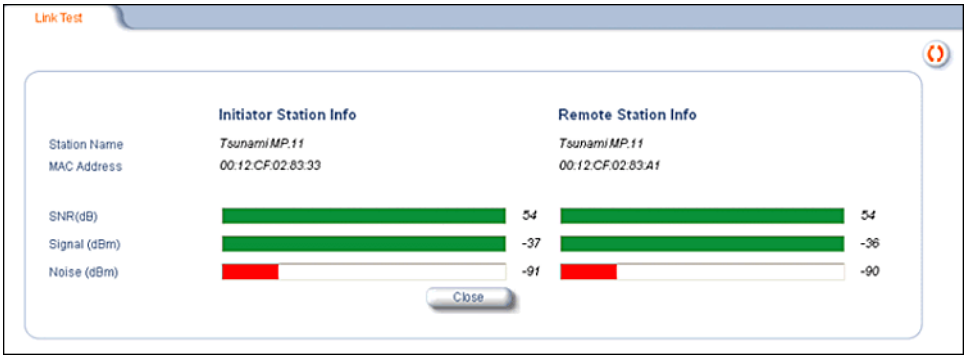
Link Test for the unit reports the Signal-to-Noise Ratio (SNR) value in dB; the higher this number, the better the signal quality. Furthermore, it reports the signal level and noise level in dBm. The latter two are approximations of the level at which the unit receives the signal of the peer unit and the background noise.

- Clicking **Explore** from a BSU displays all its registered SUs.
- Clicking **Explore** from an SU displays only the BSU with which it is registered.



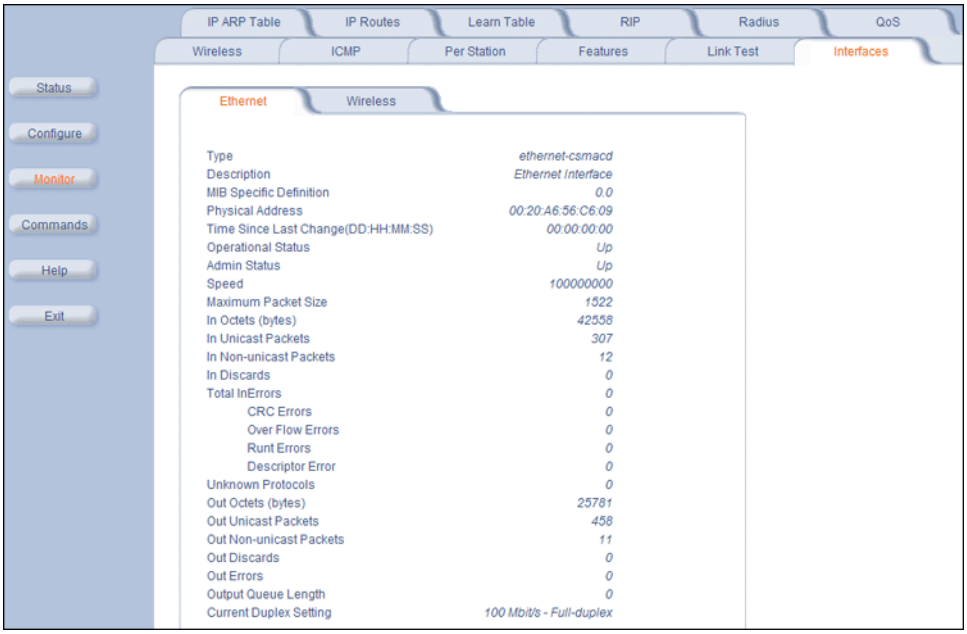
All stations displayed after “Explore” come up “Disabled.” Select a station by changing **Disabled** to **Start** and click the **Link Test** button. You can change multiple stations to **Start**, but only the last station in the list is displayed as the remote partner when you click the **Link Test** button.

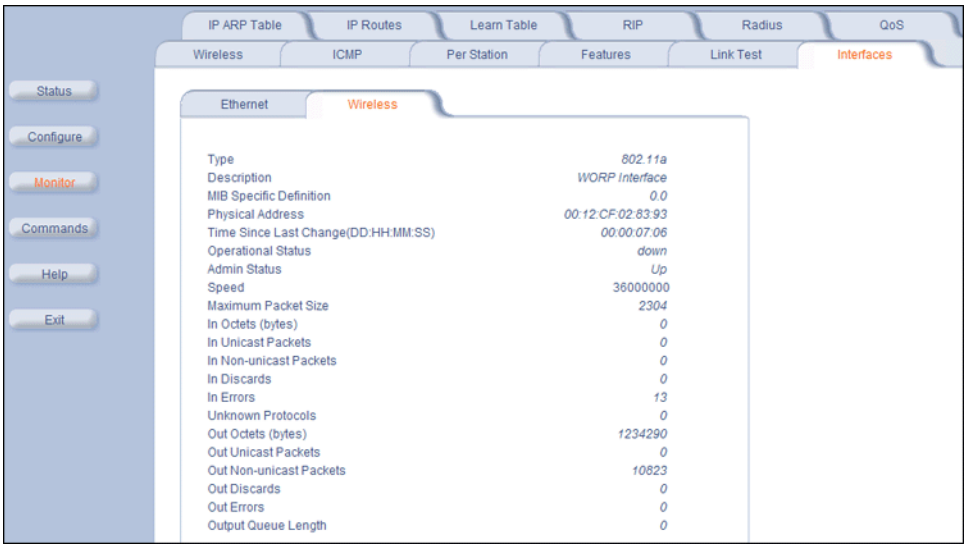
The Link Test provides SNR, Signal, and Noise information for both, the local and the remote unit’s levels. Link Test stops when you close the **Link Test** page.



Interfaces

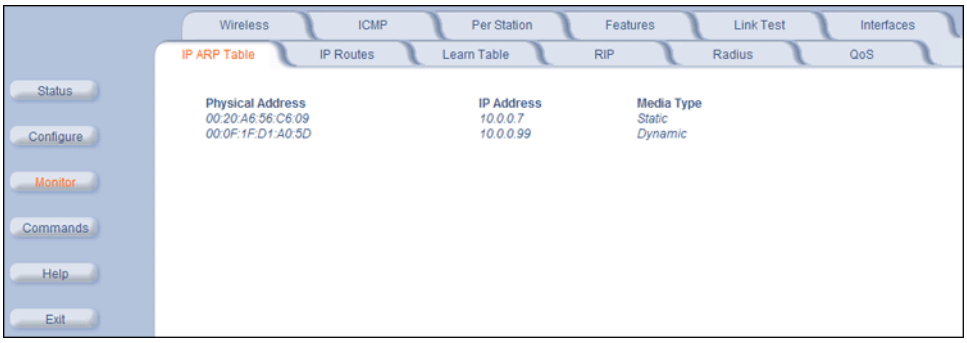
Click **Monitor** > **Interfaces** to view detailed information about the IP-layer performance of the unit's interfaces. There are two sub-tabs: **Wireless** and **Ethernet**. The following figures show both interfaces.





IP ARP Table

Click **Monitor** > **IP ARP Table** to view the mapping of the IP and MAC addresses of all radios registered at the BSU. This information is based upon the Address Resolution Protocol (ARP).

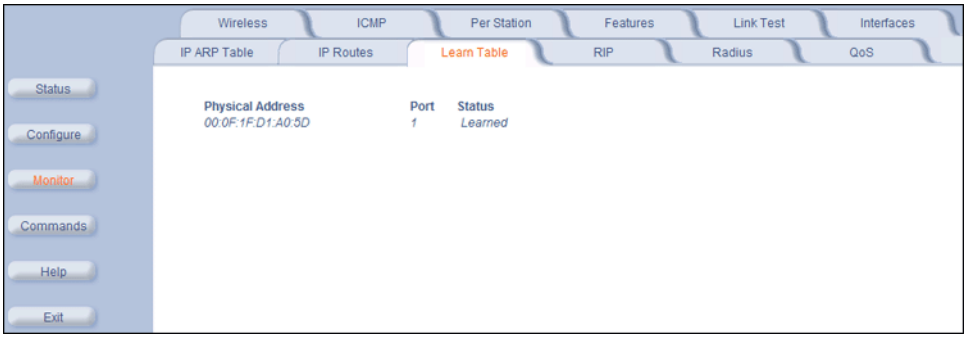


IP Routes

Click **Monitor** > **IP Routes** to view all active IP routes of the unit. These can be either **static** or **dynamic** (obtained through RIP). This tab is available only in **Routing** mode, and you can add routes only when in **Routing** mode.

Learn Table

Click **Monitor** > **Learn Table** to view all MAC addresses the unit has detected on an interface. The Learn Table displays information relating to network bridging. It reports the MAC address for each node that the device has learned is on the network and the interface on which the node was detected. There can be up to 10,000 entries in the Learn Table. This tab is only available in **Bridge** mode.

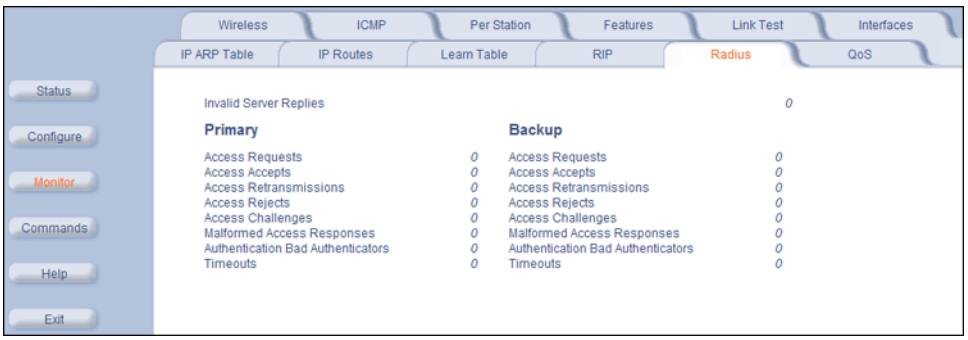


RIP

Click **Monitor** > **RIP** to view Routing Internet Protocol data for the Ethernet and Wireless interfaces.

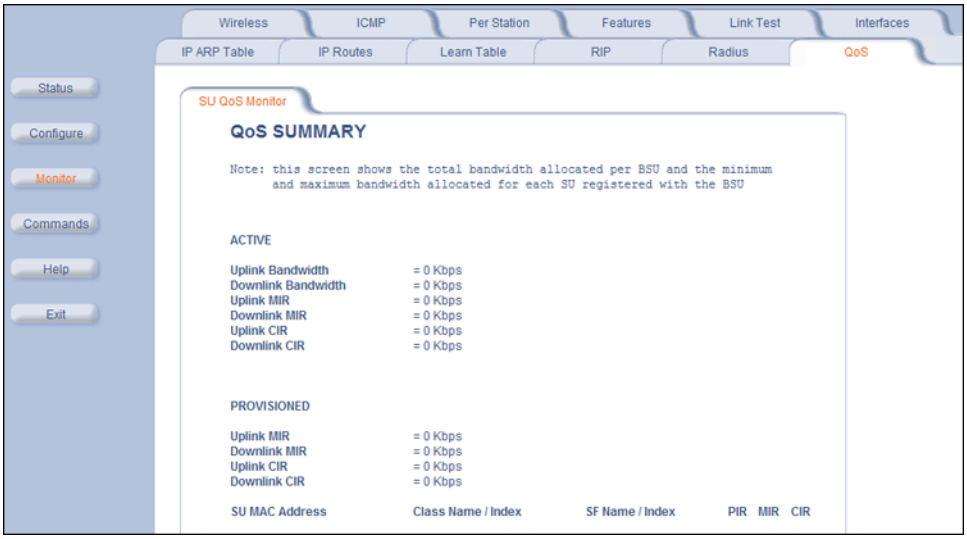
RADIUS (BSU Only)

Click **Monitor** > **Radius** to view information about the traffic exchanged with a RADIUS server.



QoS (BSU Only)

Click **Monitor** > **QoS** to view summary information about the Quality of Service per BSU and for each SU registered with that BSU.



8 Commands

This chapter describes the commands that you can issue with the Web Interface.

Click the **Commands** button to access available commands. See the following:

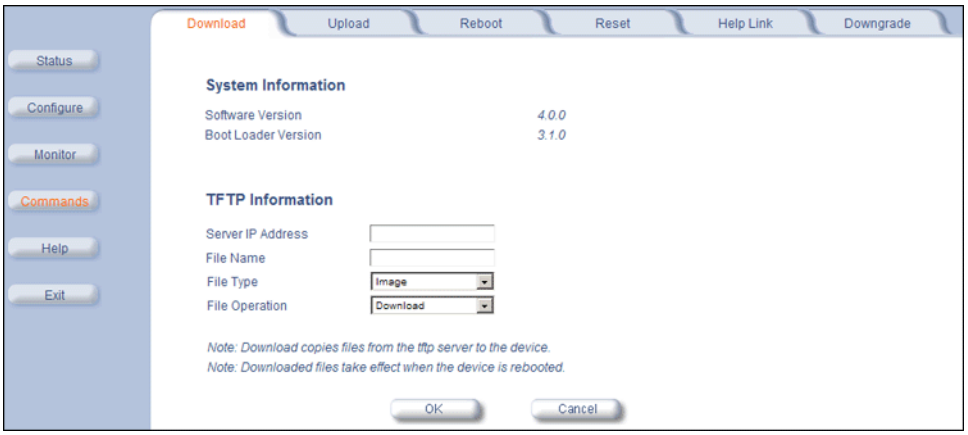
- Download
- Upload
- Reboot
- Reset
- Help Link
- Downgrade

Help and Exit buttons also appear on each page of the Web interface; click the **Help** button to access online help; click the **Exit** button to exit the application.

For an introduction to the basics of management, see Basic Management.

Download

Click **Commands** > **Download** tab to download configuration, image and license files to the unit via a TFTP server (see TFTP Server Setup for information about the SolarWinds TFTP server software located on your product installation CD).



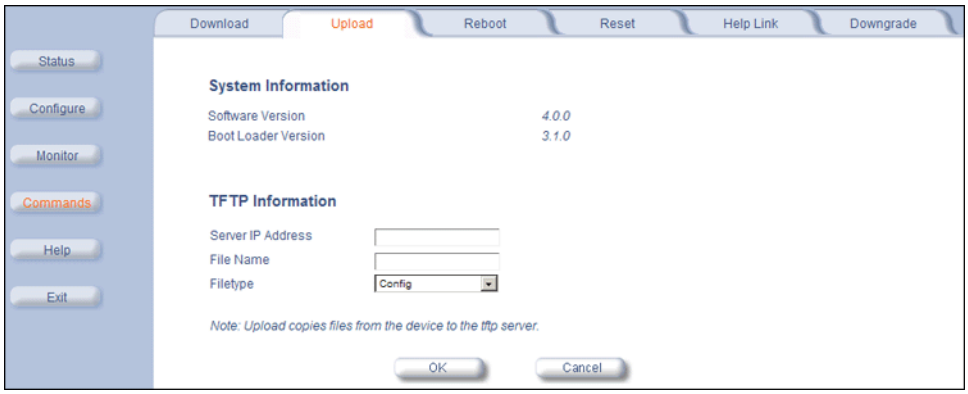
Enter the following information:

- **Server IP address:** Enter the TFTP Server IP address.
- **File Name:** Enter the name of the file to be downloaded. If you are using the SolarWinds TFTP server software located on your product installation CD, the default directory for downloading files is C:\TFTP-Root."
- **File Type:** Choose either **Config, Image, BspBl,** or **License.**
- **File Operation:** Choose either **Download** or **Download and Reboot.**

Click **OK** to start the download.

Upload

Click **Commands > Upload** to upload a configuration or log file from the unit to a TFTP server (see TFTP Server Setup for information about the SolarWinds TFTP server software located on your product installation CD).



Enter the following information:

- **Server IP address:** Enter the TFTP Server IP address.
- **File Name:** Enter the name of the file to be uploaded. If you are using the SolarWinds TFTP server software located on your product installation CD, the default directory for uploading files is C:\TFTP-Root.
- **File Type:** Choose either **Config** or **Eventlog**.

Click **OK** to start the upload.

Reboot

Click **Commands** > **Reboot** to reboot the unit's embedded software. Configuration changes are saved and the unit is reset.

CAUTION: *Rebooting the unit causes all users currently connected to lose their connection to the network until the unit has completed the reboot process and resumed operation.*

Reset

Click **Commands** > **Reset** to restore the configuration of the unit to the factory default values.

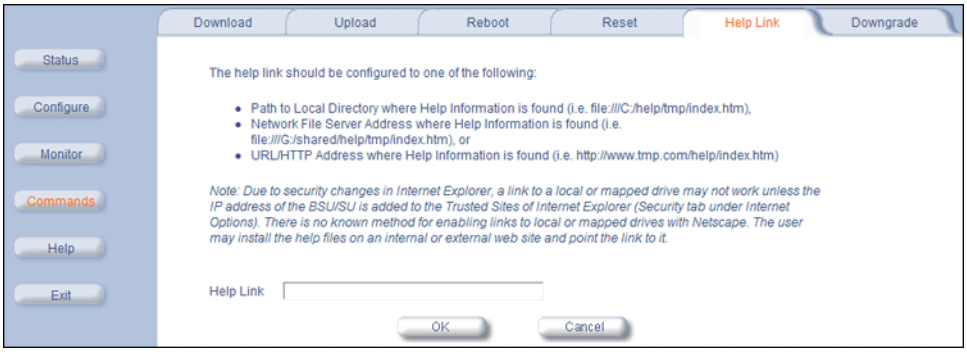
You can also reset the unit by pressing the RELOAD button located on the side of the unit. See Hard Reset to Factory Default for more information.

CAUTION: *Resetting the unit to its factory default configuration permanently overwrites all changes made to the unit. The unit reboots automatically after this command has been issued.*

Help Link

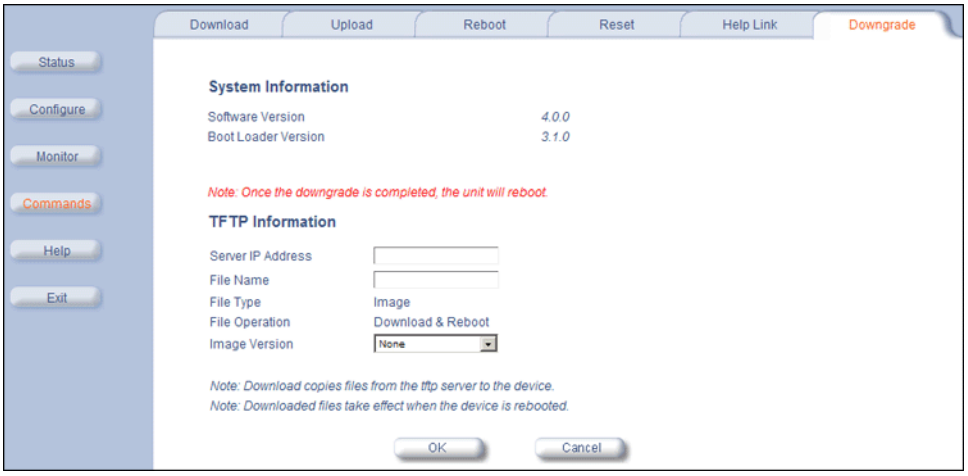
Click **Commands** > **Help Link** to set the location of the help files of the Web Interface. Upon installation, the help files are installed in the **C:\Program Files\Tsunami\MP.11 5054\Help** folder.

If you want to place these files on a shared drive, copy the **Help** folder to the new location and specify the new path in the **Help Link** box.


Download
Upload
Reboot
Reset
Help Link
Downgrade
Status
Configure
Monitor
Commands
Help
Exit
The help link should be configured to one of the following:
Path to Local Directory where Help Information is found (i.e. file:///C:/help/tmp/index.htm),
Network File Server Address where Help Information is found (i.e. file:///G:/shared/help/tmp/index.htm), or
URL/HTTP Address where Help Information is found (i.e. http://www.tmp.com/help/index.htm)
Note: Due to security changes in Internet Explorer, a link to a local or mapped drive may not work unless the IP address of the BSU/SU is added to the Trusted Sites of Internet Explorer (Security tab under Internet Options). There is no known method for enabling links to local or mapped drives with Netscape. The user may install the help files on an internal or external web site and point the link to it.
Help Link
OK
Cancel

Downgrade

Click **Commands** > **Downgrade** to downgrade to a previous release. Downgrade currently is supported only to release 2.0.1 and later. Once you enter this command, the unit is downgraded to the specified release and is automatically rebooted. The filename specified and the filename of the image selected for downgrade must be the same version. The unit will download the file, re-format the configuration to match the version, and reboot to put the image into effect.



9 Procedures

This chapter describes the following procedures:

- TFTP Server Setup: Prepares the TFTP server for transferring files to and from the unit. This procedure is used by the other procedures that transfer files.
- Web Interface Image File Download: Upgrades the embedded software.
- Configuration Backup: Saves the configuration of the unit.
- Configuration Restore: Restores a previous configuration through configuration file download.
- Soft Reset to Factory Default: Resets the unit to the factory default settings through the Web or Command Line Interface.
- Hard Reset to Factory Default: In some cases, it may be necessary to revert to the factory default settings (for example, if you cannot access the unit or you lost the password for the Web Interface).
- Forced Reload: Completely resets the unit and erases the embedded software. Use this procedure only as a last resort if the unit does not boot and the “Hard Reset to Factory Default” procedure did not help. If you perform a Forced Reload, you must download a new image file as described in Image File Download with the Bootloader.
- Image File Download with the Bootloader: If the unit does not contain embedded software, or the embedded software is corrupt, you can use this procedure to download a new image file.

TFTP Server Setup

A Trivial File Transfer Protocol (TFTP) server lets you transfer files across a network. You can upload files from the unit for backup or copying, and you can download the files for configuration and image upgrades. The SolarWinds TFTP server software is located on the product installation CD, or can be downloaded from http://support.proxim.com. You can also download the latest TFTP software from SolarWind's Web site at http://www.solarwinds.net. **The instructions that follow assume that you are using the SolarWinds TFTP server software**; other TFTP servers may require different configurations.

NOTE: *If a TFTP server is not available in the network, you can perform similar file transfer operations using the HTTP interface.*

To download or upload a file, you must connect to the computer with the TFTP server through the unit's Ethernet port. This can be any computer in the network or a computer connected to the unit with a cross-over Ethernet cable. For information about installing the TFTP server, see Step 11: Install Documentation and Software.

Ensure that:

1. The upload or download directory is correctly set (the default directory is **C:\TFTP-Root**).
2. The required image file is present in the directory.
3. The TFTP server is running. ***The TFTP server must be running only during file upload and download.*** You can check the connectivity between the unit and the TFTP server by pinging the unit from the computer that hosts the TFTP server. The ping program should show replies from the unit.
4. The TFTP server is configured to both Transmit and Receive files (on the Security tab under **File** > **Configure**), with no automatic shutdown or time-out (on the Auto-Close tab).

Web Interface Image File Download

In some cases, it may be necessary to upgrade the embedded software of the unit by downloading an image file. To download an image file through the Web Interface:

1. Set up the TFTP server as described in TFTP Server Setup.
2. Access the unit as described in Logging in to the Web Interface.
3. Click **Commands** > **Download** tab.
4. Fill in the following details:
   - **Server IP Address:** <IP address TFTP server>
   - **File Name**: <image file name>
   - **File Type:** Image
   - **File Operation:** Download
5. Click **OK** to start the file transfer.

The unit downloads the image file. The TFTP server program should show download activity after a few seconds. When the download is complete, the unit is ready to start the embedded software upon reboot.

Configuration Backup

You can back up the unit's configuration by uploading the configuration file. You can use this file to restore the configuration or to configure another unit (see Configuration Restore).

To upload a configuration file through the Web Interface:

1. Set up the TFTP server as described in TFTP Server Setup.
2. Access the unit as described in Logging in to the Web Interface.
3. Click **Commands** > **Upload**.
4. Fill in the following details:
   - **Server IP Address:** <IP address TFTP server>
   - **File Name:** <configuration file name>
   - **File Type:** Config
   - **File Operation:** Upload
5. Click **OK** to start the file transfer.

The unit uploads the configuration file. The TFTP server program should show upload activity after a few seconds. When the upload is complete, the configuration is backed up.

Configuration Restore

You can restore the configuration of the unit by downloading a configuration file. The configuration file contains the configuration information of a unit.

To download a configuration file through the Web Interface:

1. Set up the TFTP server as described in TFTP Server Setup.
2. Access the unit as described in Logging in to the Web Interface.
3. Click **Commands** > **Download** tab.
4. Fill in the following details:
   - **Server IP Address:** <IP address TFTP server>
   - **File Name:** <configuration file name>
   - **File Type:** Config
   - **File Operation:** Download
5. Click **OK** to start the file transfer.

The unit downloads the configuration file. The TFTP server program should show download activity after a few seconds. When the download is complete and the system rebooted, the configuration is restored.

Soft Reset to Factory Default

If necessary, you can reset the unit to the factory default settings. Resetting to default settings means that you must configure the unit anew.

To reset to factory default settings using the Web Interface:

1. Click **Commands** > **Reset**.
2. Click the **Reset to Factory Default** button.

The device configuration parameter values are reset to their factory default values.

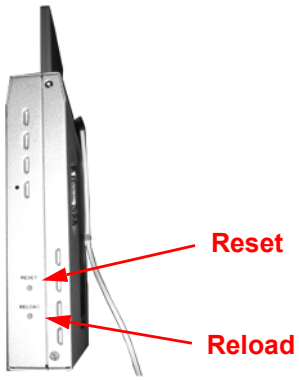
If you do not have access to the unit, you can use the procedure described in Hard Reset to Factory Default below as an alternative.

Hard Reset to Factory Default

If you cannot access the unit's user interface or you have lost its password, you can reset the unit to the factory default settings. Resetting to default settings means you must configure the unit anew.

To reset to factory default settings, using the end of a paper clip, press and hold the unit's **RELOAD** button for a minimum of 5 seconds but no more than 10 seconds. The configuration is deleted from the unit and the unit reboots, writing and using a default configuration.

CAUTION: *It you hold the RELOAD button for longer than 20 seconds, you may go into* Forced Reload *mode, which erases the unit's embedded software. This software image must be reloaded through an Ethernet connection with a TFTP server. The image filename to be downloaded can be configured with either ScanTool through the Ethernet interface or with the Boot Loader CLI through the serial port to make the unit functional again.*



Forced Reload

With Forced Reload, you erase the embedded software. Use this procedure only as a last resort if the unit does not boot and the “Reset to Factory Defaults” procedure did not help. If you perform a Forced Reload, you must download a new image file with the Bootloader (see “Image File Download with the Bootloader” below).

CAUTION: *The following procedure erases the embedded software of the unit. This software image must be reloaded through an Ethernet connection with a TFTP server. The image filename to be downloaded can be configured with ScanTool through the Ethernet interface to make the unit functional again.*

To do a forced reload:

1. Press and release the **RESET** button on the 5054 unit; the unit resets and the LEDs flash.
2. Immediately press and hold the **RELOAD** button for about 20 seconds. The software image and configuration are deleted from the unit.
3. Follow the Image File Download with the Bootloader procedure to download an image file.

Image File Download with the Bootloader

The following procedures download an image file to the unit after the embedded software has been erased with Forced Reload or when the embedded software cannot be started by the Bootloader. A new image file can be downloaded to the unit via ScanTool or via the Command Line Interface through the unit's serial port. In both cases, the file is transferred through Ethernet with TFTP. Because the CLI serial port option requires a serial RS-232C cable, Proxim recommends the ScanTool option.

Download with ScanTool

To download an image file with the ScanTool:

1. Set up the TFTP server as described in TFTP Server Setup.
2. Run ScanTool on a computer that is connected to the same LAN subnet as the unit. ScanTool scans the subnet for units and displays the found units in the main window. If in Forced Reload, ScanTool does not find the device until the unit Bootloader times out from its default operation to download an image. Click **Rescan** to re-scan the subnet and update the display until the unit shows up in Bootloader mode.
3. Select the unit to which you want to download an image file and click Change.
4. Ensure that **IP Address Type Static** is selected and fill in the following details:
   - Password
   - IP Address and Subnet Mask of the unit.
   - **TFTP Server IP Address** and, if necessary, the **Gateway IP Address** of the TFTP server.
   - **Image File Name** of the file with the new image.
5. Click **OK** to start the file transfer.

The unit downloads the image file. The TFTP server program should show download activity after a few seconds. When the download is complete, the LED pattern should return to **reboot** state. The unit is ready to start the embedded software.

After a Forced Reload procedure, the unit returns to factory default settings and must be reconfigured. ScanTool can be used to set the system name and IP address.

To access the unit, see Logging in to the Web Interface.

Download with CLI

To use the CLI through the serial port of the 5054 you need a serial RS-232C cable with a male and a female DB9 connector, and an ASCII terminal program such as HyperTerminal. Proxim recommends you switch off the 5054 and the computer before connecting or disconnecting the serial RS-232C cable.

To download an image file:

1. Set up the TFTP server as described in TFTP Server Setup.
2. Start the terminal program (such as HyperTerminal), set the following connection properties, and then connect:
   - COM port: for example, COM1 or COM2 to which the unit serial port is connected)
   - Bits per second: 9600
   - Data bits: 8
   - Stop bits: 1
   - Flow control: None
   - Parity: None
3. Disconnect and reconnect power or press the RESET button to reset the unit; the terminal program displays Power On Self Test (POST) messages.

4. When the **"Sending Traps to SNMP manager periodically**" message is displayed (after about 30 seconds), press the **ENTER** key.
5. The command prompt is displayed; enter the following commands:

```
set ipaddr <IP address nit>
set ipsubmask <subnet mask>
set ipaddrtype static
set tftpipaddr <IP address TFTP server>
set tftpfilename <image file name>
set ipgw <gateway IP address>
reboot
```

For example:

```
set ipaddr 10.0.0.12
set ipsubmask 255.255.255.0
set ipaddrtype static
set tftpipaddr 10.0.0.20
set tftpfilename image.bin
set ipgw 10.0.0.30
reboot
```

The unit reboots and downloads the image file. The TFTP server program should show download activity after a few seconds. When the download is complete, the unit is ready for configuration.

To access the unit, see Logging in to the Web Interface. Note that the IP configuration in normal operation differs from the IP configuration of the Boot Loader.

10 Troubleshooting

This chapter helps you to isolate and solve problems with your unit. In the event this chapter does not provide a solution, or the solution does not solve your problem, check our support website at http://support.proxim.com.

Before you start troubleshooting, it is important that you have checked the details in the product documentation. For details about RADIUS, TFTP, terminal and telnet programs, and Web browsers, refer to the appropriate documentation.

In some cases, rebooting the unit clears the problem. If nothing else helps, consider a Soft Reset to Factory Default or a Forced Reload. The Forced Reload option requires you to download a new image file to the unit.

See the following:

- Connectivity Issues
- Communication Issues
- Setup and Configuration Issues
- VLAN Operation Issues
- Link Problems

Connectivity Issues

The issues described in this section relate to the connections of the unit.

Unit Does Not Boot

The unit shows no activity (the power LED is off).

1. Ensure that the power supply is properly working and correctly connected.
2. Ensure that all cables are correctly connected.
3. Check the power source.
4. If you are using an Active Ethernet splitter, ensure that the voltage is correct.

Serial Link Does Not Work

The unit cannot be reached through the serial port.

1. Check the cable connection between the unit and the computer.
2. Ensure that the correct COM port is used.
3. Start the terminal program; set the following connection properties (also see “HyperTerminal Connection Properties” in the *Tsunami MP.11/QB.11 Reference Manual*), and then connect.
   - COM port: for example, COM1 or COM2 to which the unit serial port is connected)
   - Bits per second: 9600
   - Data bits 8
   - Stop bits: 1
   - Flow control: None
   - Parity: None
4. Ensure that the unit and the computer use the same serial port configuration parameters.
5. Disconnect and reconnect power to reset the unit. The terminal program displays Power On Self Tests (POST) messages and displays the following after approximately 90 seconds: **`Please enter password`**:

HyperTerminal Connection Problems

The serial connection properties can be found in HyperTerminal as follows:

1. Start HyperTerminal and select Properties from the File menu.
2. Select **Direct to Com 1** in the **Connect using**: drop-down list (depending upon the COM port you use); then click **Configure**. A window such as the following is displayed:
3. Enter or edit the information as follows, and click **OK**.
   - Bits per second: 9600
   - Data bits: 8
   - Parity: None
   - Stop bits: 1
   - Flow control: None
4. Click **Settings** > **ASCII Setup.**
5. Ensure that Send line ends with line feeds is selected and click OK twice. HyperTerminal is now correctly configured.

Ethernet Link Does Not Work

1. First check the Ethernet LED:
   - Solid Green: Power is on, the radio is up, and the Ethernet link is also up.
   - Blinking Green: Power is on, the radio is coming up and the Ethernet is down.
2. Verify pass-through versus cross-over cable.

Cannot Use the Web Interface

1. Open a command prompt window and enter **`ping <ip address unit>`** (for example **`ping 10.0.0.1`**). If the unit does not respond, make sure that you have the correct IP address.
   If the unit responds, the Ethernet connection is working properly, continue with this procedure.
2. Ensure that you are using one of the following Web browsers:
   - Microsoft Internet Explorer version 5.0 or later (Version 6.0 or later recommended)
   - Netscape version 6.0 or later.
3. Ensure that you are not using a proxy server for the connection with your Web browser.
4. Ensure that you have not exceeded the maximum number of Web Interface or CLI sessions.
5. Double-check the physical network connections. Use a well-known unit to ensure the network connection is properly functioning.
6. Perform network infrastructure troubleshooting (check switches, routers, and so on).

Communication Issues

Two Units Are Unable to Communicate Wirelessly

If a wireless link is possible after testing two units within close distance of each other, then there are two possible reasons why wireless connectivity is not possible while the MP.11 units are at their desired locations:

1. There may be a problem in the RF path, for example, a bad connector attachment (this is the most common problem in installations) or a bad cable (water ingress).

   NOTE: *The cables can be swapped with known good ones as a temporary solution to verify cable quality.*

2. Another reason may be related to an interference problem caused by a high signal level from another radio. This can be checked by changing the frequency and then verifying whether another channel works better or by changing the polarization as a way of avoiding the interfering signal. To know in advance how much interference is present in a given environment, a Spectrum Analyzer can be attached to a (temporary) antenna for measuring the signal levels on all available Channels.

NOTE: *The antennas are usually not the problem, unless mounted upside down causing the drain hole to be quickly filled with radome.*

If a wireless link is not possible after testing two units within close distance of each other, then the problem is either hardware or configuration related, such as a wrong Network name, Encryption key, Network Secret or Base Station Name. To eliminate these issues from being a factor, resetting the both units to factory defaults is the recommended solution.

If a wireless link is not possible after resetting the units and verifying that one unit is a BSU with WORP Base interface configured and the other is a Satellite, then the problem is not configuration related and the only remaining reason is a possible hardware problem. Acquiring a third unit and then testing it amongst the existing units will help pinpoint the broken unit.

Setup and Configuration Issues

The following issues relate to setup and configuration problems.

Lost Password

If you lost your password, you must reset the unit to the default settings. See Hard Reset to Factory Default. The default password is **public**.

If you record your password, keep it in a safe place.

The Unit Responds Slowly

If the unit takes a long time to become available, it could mean that:

- No DHCP server is available.
- The IP address of the unit is already in use.

  Verify that the IP address is assigned only to the unit. Do this by switching off the unit and then pinging the IP address. If there is a response to the ping, another device in the network is using the same IP address. If the unit uses a static IP address, switching to DHCP mode could remedy this problem. Also see Setting the IP Address with ScanTool.
- There is too much network traffic.

Web Interface Does Not Work

If you cannot connect to the unit Web server through the network:

1. Connect a computer to the serial port of the unit and check the HTTP status. The HTTP status can restrict HTTP access at different interfaces. For more information, see “Serial Port” in the *Tsunami MP.11/QB.11 Reference Manual*.
2. Open a command prompt window and enter: **`ping <ip address unit>`** (for example **`ping 10.0.0.1`**)
   - If the unit does not respond, ensure that you have the correct IP address.
   - If the unit responds, the Ethernet connection is working properly; continue with this procedure.
3. Ensure that you are using one of the following Web browsers:
   - Microsoft Internet Explorer version 5.0 or later (Version 6.0 or later recommended)
   - Netscape version 6.0 or later
4. Ensure that you are not using a proxy server for the connection with your Web browser.
5. Ensure that you have not exceeded the maximum number of Web Interface sessions.

Command Line Interface Does Not Work

If you cannot connect to the unit through the network:

1. Connect a computer to the serial port of the unit and check the SNMP table. The SNMP table can restrict telnet or HTTP access. For more information, see “Serial Port” in the *Tsunami MP.11/QB.11 Reference Manual*.
2. Open a command prompt window and enter: **`ping`** `<ip address unit>` (for example **`ping 10.0.0.1`**).
   - If the unit does not respond, ensure that you have the correct IP address.
   - If the unit responds, the Ethernet connection is working properly; continue with this procedure.
3. Ensure that you have not exceeded the maximum number of CLI sessions.

TFTP Server Does Not Work

With TFTP, you can transfer files to and from the unit. Also see TFTP Server Setup. If a TFTP server is not properly configured and running, you cannot upload and download files. The TFTP server:

- Can be situated either local or remote
- Must have a valid IP address
- Must be set for send and receive without time-out
- Must be running only during file upload and download

If the TFTP server does not upload or download files, it could mean:

- The TFTP server is not running
- The IP address of the TFTP server is invalid
- The upload or download directory is not correctly set
- The file name is not correct

Online Help Is Not Available

Online help is not available:

1. Make sure that the Help files are installed on your computer or server. Also see Step 11: Install Documentation and Software.
2. Verify whether the path of the help files in the Web Interface refers to the correct directory. See Help Link.

Changes Do Not Take Effect

Changes made in the Web Interface do not take effect:

1. Restart your Web browser.
2. Log into the radio unit again and make changes.
3. Reboot the radio unit when prompted to do so.

Wait until the reboot is completed before accessing the unit again.

VLAN Operation Issues

The correct VLAN configuration can be verified by “pinging” wired hosts from both sides of the device and the network switch. Traffic can be “sniffed” on the wired (Ethernet) network. Packets generated by hosts and viewed on one of the backbones should contain IEEE 802.1Q compliant VLAN headers when in Transparent mode. The VLAN ID in the headers should correspond to one of the VLAN Management IDs configured for the unit in Trunk mode.

The correct VLAN assignment can be verified by pinging:

- The unit to ensure connectivity
- The switch to ensure VLAN properties
- Hosts past the switch to confirm the switch is functional

Ultimately, traffic can be “sniffed” on the Ethernet interface using third-party packages. Most problems can be avoided by ensuring that 802.1Q compliant VLAN tags containing the proper VLAN ID have been inserted in the bridged frames. The VLAN ID in the header should correspond to the assigned VLAN.

What if network traffic is being directed to a nonexistent host?

- All sessions are disconnected, traffic is lost, and a manual override is necessary.
- Workaround: You can configure the switch to mimic the nonexistent host.

Link Problems

While wireless networking emerges more and more, the number of wireless connections to networks grows every day. The Tsunami MP.11 unit is one of the successful product families used by customers today who enjoy the day after day high-speed, cost-effective connections. To successfully use the connections, technicians must be able to troubleshoot the system effectively. This section gives hints on how a unit network could be analyzed in the case of “no link,” a situation in which the customer thinks that the link is down because there is no traffic being passed.

The four general reasons that a wireless link may not work are related to:

- Hardware
- Configuration
- Path issues (such as distance, cable loss, obstacles)
- Environment (anything that is outside the equipment and not part of the path itself)

You have tested the equipment in the office and have verified that the hardware and configurations are sound. The path calculation has been reviewed, and the path has been double-checked for obstacles and canceling reflections. Still, the user reports that the link does not work.

Most likely, the problem reported is caused by the environment or by improper tests to verify the connection. This article assumes that the test method, cabling, antennas, and antenna alignment have been checked. Always do this before checking the environment.

General Check

Two general checks are recommended before taking any action:

- Check whether the software version at both sides is the most current
- Check for any reported alarm messages in the Event Log

Statistics Check

Interference and other negative environment factors always have an impact on the number of correctly received frames. The Tsunami MP.11 models give detailed information about transmission errors in the Web interface, under **Monitor**.

The windows that are important for validating the health of the link are:

- **Monitor / Wireless / General (Lowest level of the wireless network):** Check FCS errors: Rising FCS errors indicate interference or low fade margin. So does **Failed count**. If only one of those is high, this indicates that a source of interference is significant near one end of the link.
- **Monitor / Interfaces / Wireless (One level higher than Wireless / General):** The information is given after the wireless Ethernet frame is converted into a normal Ethernet frame. The parameters shown are part of the MIB-II.
  - Both operational and admin status should be **up**. An admin status of **down** indicates that the interface is configured to be down.
  - **In Discards** and **Out Discards** indicate overload of the buffers, likely caused by network traffic, which is too heavy.
  - **In Errors** and **Out Errors** should never happen; however, it might happen if a frame’s FCS was correct while the content was still invalid.
- **Monitor / Wireless / WORP (Statistics on WORP):** WORP runs on top of normal Ethernet, which means that the WORP frame is in fact the data field of the Ethernet frame. **Send Failure** or **Send Retries** must be low in comparison to **Send Success**. **Low** is about 1%. The same applies for **Receive Success** versus **Receive Retries** and **Receive Failures**. Note that the **Receive Failures** and **Retries** can be inaccurate. A frame from the remote site might have been transmitted without even being received; therefore, the count of that frame might not have been added to the statistics and the receiver simply could not know that there was a frame.

  - **Remote Partners** indicates how many SUs are connected (in case of a BSU) or whether a Base is connected (in case of a Subscriber).
  - **Base Announces** should increase continuously.
  - **Registration Requests** and **Authentication Requests** should be divisible by 3. WORP is designed in a way that each registration sequence starts with 3 identical requests. It is not a problem if, once in a while, one of those requests is missing. Missing requests frequently is to be avoided.
- **Monitor / Per Station (Information per connected remote partner):** Check that the received signal level (RSL) is the same on both sides; this should be the case if output power is the same. Two different RSLs indicate a broken transmitter or receiver. A significant difference between Local Noise and Remote Noise could indicate a source of interference near the site with the highest noise. Normally, noise is about –80 dBm at 36 Mbps. This number can vary from situation to situation, of course, also in a healthy environment.
- **Monitor / Link Test (Information used by Administrators for on-the-spot checking):** Check the received signal level (RSL) and noise level. Compare the RSL with the values from path analysis. If the figures differ significantly from the values recorded at the Per Station window, check for environment conditions that change over time.

Analyzing the Spectrum

The ultimate way to discover whether there is a source of interference is to use a spectrum analyzer. Usually, the antenna is connected to the analyzer when measuring. By turning the antenna 360 degrees, one can check from which direction the interference is coming. The analyzer will also display the frequencies and the level of signal is detected.

Proxim recommends performing the test at various locations to find the most ideal location for the equipment.

Avoiding Interference

When a source of interference is identified and when the level and frequencies are known, the next step is to avoid the interference. Some of the following actions can be tried:

- Changing the channel to a frequency away from the interference is the first step in avoiding interference. The installer can select a **DFS Preferred Channel**.
- Each antenna has a polarization; try to change to a polarization different from the interferer.
- A small beam antenna looks only in one particular direction. Because of the higher gain of such an antenna, lowering the output power or adding extra attenuation might be required to stay legal. This solution cannot help when the source of interference is right behind the remote site.
- Lowering the antennas can help avoid seeing interference from far away.

Move the antennas to a different location on the premises. This causes the devices to look from a different angle, causing a different pattern in the reception of the signals. Use obstructions such as buildings, when possible, to shield from the interference.

Conclusion

A spectrum analyzer can be a great help to identify whether interference might be causing link problems on Tsunami MP.11 systems.

Before checking for interference, the link should be verified by testing in an isolated environment, to make sure that hardware works and your configurations are correct. The path analysis, cabling and antennas should be checked as well.

Statistics in the web interface under Monitor tell if there is a link, if the link is healthy, and a continuous test can be done using the Link Test.

Country Codes and Channels

A

In the CLI and MIB browser, the country code is set using the string code, as shown in the following example.

Example: To set Taiwan as the country:

```
set syscountrycode TW
```

NOTE: *The country code must be entered in capital letters.*

Channels/Frequencies by Country

Country (Code)	Frequency Bands	DFS	Allowed Channels (Center Freq)
All Channels - 5 GHz (A5)	All 5 GHz bands	No	All 20 MHz channels.
Argentina (AR)	5.25 - 5.35 GHz and 5.725 - 5.825 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805)
Australia (AU)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Austria (AT)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Belgium (BE)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Belize (BZ)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Bolivia (BO)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Brazil (BR)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Brazil 5.8 GHz (B1)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Brunei Darussalam (BN)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Bulgaria (BG)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Canada (CA)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Canada DFS (C1)	5.25 - 5.35 GHz and 5.47 - 5.725 GHz	Yes	**56** (5280), **60** (5300), **64** (5320), **100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
China (CN)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Colombia (CO)	5.25 - 5.35 GHz and 5.725 - 5.85 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Cyprus (CY)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Czech Republic	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Denmark (DK)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Dominican Republic (DO)	5.25 - 5.35 GHz and 5.725 - 5.85 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Estonia (EE)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Finland (FI)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
France (FR)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)

Country (Code)	Frequency Bands	DFS	Allowed Channels (Center Freq)
Germany (DE)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Greece (GR)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Guatemala (GT)	5.25 - 5.35 GHz and 5.725 - 5.85 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Hong Kong (HK)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Hungary (HU)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Iceland (IS)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
India (IN)	5.15 - 5.35 GHz and 5.725 - 5.870 GHz	No	**36** (5180), **40** (5200), **44** (5220), **48** (5240), **52** (5260), **56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825), **169** (5845), **173** (5865)
Iran (IR)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Ireland (IE)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Ireland 5.8 GHz (I1)	5.725 - 5.85 GHz	Yes	**147** (5735), **151** (5755), **155** (5775), **167** (5835)
Italy (IT)	5.47 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Japan (JP)	5.25 - 5.35 GHz	Yes	**56** (5280), **60** (5300), **64** (5320)
Japan2 (J2)	5.15 - 5.25 GHz	No	**34** (5170), **38** (5190), **42** (5210), **46** (5230)
Korea Republic (KR)	5.725 - 5.825 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805)
Korea Republic2 (K2)	5.725 - 5.825 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805)
Latvia (LV)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Liechtenstein (LI)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Lithuania (LT)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Luxembourg (LU)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Macau (MO)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Malaysia (MY)	5.25 - 5.35 GHz and 5.725 - 5.85 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Malta (MT)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Mexico (MX)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Netherlands (NL)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
New Zealand (NZ)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
North Korea (KP)	5.725 - 5.825 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805)
Norway (NO)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Panama (PA)	5.25 - 5.35 GHz and 5.725 - 5.85 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Philippines (PH)	5.25 - 5.35 GHz and 5.725 - 5.85 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Poland (PL)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Portugal (PT)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)

Country (Code)	Frequency Bands	DFS	Allowed Channels (Center Freq)
Puerto Rico (PR)	5.25 - 5.35 GHz and 5.725 - 5.85 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Russia (RU)	5.15 - 6.08 GHz	No	**30** (5150), **34** (5170), **38** (5190), **42** (5210), **46** (5230), **50** (5250), **54** (5270), **58** (5290), **62** (5310), **66** (5330), **70** (5350), **74** (5370), **78** (5390), **82** (5410), **86** (5430), **90** (5450), **94** (5470), **98** (5490), **102** (5510), **106** (5530), **110** (5550), **114** (5570), **118** (5590), **122** (5610), **126** (5630), **130** (5650), **134** (5670), **138** (5690), **142** (5710), **146** (5730), **150** (5750), **154** (5770), **158** (5790), **162** (5810), **166** (5830), **170** (5850), **174** (5870), **178** (5890), **182** (5910), **186** (5930), **190** (5950), **194** (5970), **198** (5990), **202** (6010), **206** (6030), **210** (6060), **214** (6070)
Saudi Arabia (SA)	5.15 - 5.35 GHz and 5.725 - 5.825 GHz	No	**36** (5180), **40** (5200), **44** (5220), **48** (5240), **52** (5260), **56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805)
Singapore (SG)	5.15 - 5.25 GHz and 5.725 - 5.85 GHz	No	**36** (5180), **40** (5200), **44** (5220), **48** (5240), **149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
Slovak Republic (SK)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Slovenia (SI)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
South Africa (ZA)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Spain (ES)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Sweden (SE)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Switzerland (CH)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Taiwan (158)	5.25 - 5.35 GHz and 5.725 - 5.825 GHz	No	**56** (5280), **60** (5300), **64** (5320), **149** (5745), **153** (5765), **157** (5785), **161** (5805)
Thailand (TH)	5.725 - 5.825 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805)
United Kingdom (GB)	5.47 - 5.725 GHz	Yes	**100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
United Kingdom 5.8 GHz (G1)	5.725 - 5.85 GHz	Yes	**147** (5735), **151** (5755), **155** (5775), **167** (5835)
United States (US)	5.725 - 5.85 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805), **165** (5825)
United States DFS (U1)	5.25 - 5.35 GHz and 5.47 - 5.725 GHz	Yes	**56** (5280), **60** (5300), **64** (5320), **100** (5500), **104** (5520), **108** (5540), **112** (5560), **116** (5580), **120** (5600), **124** (5620), **128** (5640), **132** (5660), **136** (5680), **140** (5700)
Uruguay (UY)	5.725 - 5.825 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805)
Venezuela (VE)	5.725 - 5.825 GHz	No	**149** (5745), **153** (5765), **157** (5785), **161** (5805)

B

Technical Specifications

Please see the following sections:

- Part Numbers
- Regulatory Approval and Frequency Ranges
- OFDM Modulation Rates
- Wireless Protocol
- Interfaces
- Receive Sensitivity
- Maximum Throughput
- Latency
- Transmit Power Settings
- Range Information
- Hardware Specifications
- Software Features
- Management
- LEDs
- Power Requirements
- Physical and Environmental Specifications
- MTBF and Warranty

Part Numbers

Radio Units

North America Region

Base Station Unit

Part Number	Description
5054-BSU-US	Tsunami MP.11 Model 5054 (MP.11a) Base Station Unit – USA/CAN PSU

Residential Subscriber Unit

Part Number	Description
5054-RSU-US-WA	Tsunami MP.11 5054 (MP.11a) Residential Subscriber Unit– USA/CAN PSU-w/15 dBi Window Antenna
5054-RSU-US-MP	Tsunami MP.11 5054 (MP.11a) Residential Subscriber Unit– USA/CAN PSU-5-pack*

* 5-Packs contain: RSU (5), Power Supply (5); no software, no documentation, no antennas

Subscriber Unit

Part Number	Description
5054-SU-US	Tsunami MP.11 5054 (MP.11a) Subscriber Unit– USA/CAN PSU

Europe and Middle East Regions

Base Station Unit

Part Number	Description
5054-BSU-EU	Tsunami MP.11 Model 5054 (MP.11a) Base Station Unit – Europe PSU
5054-BSU-UK	Tsunami MP.11 Model 5054 (MP.11a) Base Station Unit – UK PSU

Residential Subscriber Unit

Part Number	Description
5054-RSU-EU-WA	Tsunami MP.11 5054 (MP.11a) Residential Subscriber Unit– Europe PSU-w/15 dBi Window Antenna
5054-RSU-UK-WA	Tsunami MP.11 5054 (MP.11a) Residential Subscriber Unit– UK PSU-w/15 dBi Window

Residential Subscriber Unit 5-packs*

Part Number	Description
5054-RSU-EU-MP	Tsunami MP.11 5054 (MP.11a) Residential Subscriber Unit– Europe PSU-5 pack
5054-RSU-UK-MP	Tsunami MP.11 5054 (MP.11a) Residential Subscriber Unit– UK PSU-5-pack

* 5-Packs contain: RSU (5), Power Supply (5); no software, no documentation, no antennas

Subscriber Unit

Part Number	Description
5054-SU-EU	Tsunami MP.11 Model (MP.11a) Subscriber Unit, EU PSU
5054-SU-UK	Tsunami MP.11 Model (MP.11a) Subscriber Unit, UK PSU

Asia Pacific Region

Base Station Unit

Part Number	Description
5054-BSU-EU	Tsunami MP.11 Model 5054 (MP.11a) Base Station Unit – Europe PSU
5054-BSU-UK	Tsunami MP.11 Model 5054 (MP.11a) Base Station Unit – UK PSU
5054-BSU-AU	Tsunami MP.11 Model 5054 (MP.11a) Base Station Unit – Australia PSU
5054-BSU-SK	Tsunami MP.11 Model 5054 (MP.11a) Base Station Unit – South Korea PSU
5054-BSU-CN	Tsunami MP.11 Model 5054 (MP.11a) Base Station Unit – China PSU
5054-BSU-US-WORLD	Tsunami MP.11 Model 5054 (MP.11a) Base Station Unit – US/CAN PSU - WORLD

Residential Subscriber Unit

Part Number	Description
5054-BSU-EU	Tsunami MP.11 Model 5054 (MP.11a) Residential Subscriber Unit – Europe PSU - w/ 15 dBi Window Antenna
5054-BSU-UK	Tsunami MP.11 Model 5054 (MP.11a) Residential Subscriber Unit – UK PSU - w/15 dBi Window Antenna
5054-BSU-AU	Tsunami MP.11 Model 5054 (MP.11a) Residential Subscriber Unit – Australia PSU - w/ 15 dBi Window Antenna
5054-BSU-SK	Tsunami MP.11 Model 5054 (MP.11a) Residential Subscriber Unit – South Korea PSU - w/15 dBi Window Antenna
5054-BSU-CN	Tsunami MP.11 Model 5054 (MP.11a) Residential Subscriber Unit – China PSU - w/15 dBi Window Antenna
5054-BSU-US-WORLD	Tsunami MP.11 Model 5054 (MP.11a) Residential Subscriber Unit – US/CAN PSU - w/ 15 dBi Window Antenna - World

Residential Subscriber Unit 5-packs*

Part Number	Description
5054-RSU-AU-MP	Tsunami MP.11 Model 5054 (MP.11a) Residential Subscriber Unit – Australia PSU - 5-pack
5054-RSU-US-MP-WORLD	Tsunami MP.11 Model 5054 (MP.11a) Residential Subscriber Unit – US/CAN PSU - 5-pack WORLD
5054-RSU-SK-MP	Tsunami MP.11 Model 5054 (MP.11a) Residential Subscriber Unit – South Korea PSU - 5-pack
5054-RSU-CN-MP	Tsunami MP.11 Model 5054 (MP.11a) Residential Subscriber Unit – China PSU - 5-pack
5054-RSU-EU-MP	Tsunami MP.11 Model 5054 (MP.11a) Residential Subscriber Unit – Europe PSU - 5-pack
5054-RSU-UK-MP	Tsunami MP.11 Model 5054 (MP.11a) Residential Subscriber Unit – UK PSU - 5-pack

* 5-Packs contain: RSU (5), Power Supply (5); no software, no documentation, no antennas

Subscriber Unit

Part Number	Description
5054-SU-EU	Tsunami MP.11 Model 5054 (MP.11a) Subscriber Unit – Europe PSU
5054-SU-UK	Tsunami MP.11 Model 5054 (MP.11a) Subscriber Unit – UK PSU
5054-SU-AU	Tsunami MP.11 Model 5054 (MP.11a) Subscriber Unit – Australia PSU
5054-SU-SK	Tsunami MP.11 Model 5054 (MP.11a) Subscriber Unit – South Korea PSU
5054-SU-CN	Tsunami MP.11 Model 5054 (MP.11a) Subscriber Unit – China PSU

Part Number	Description
5054-SU-US-WORLD	Tsunami MP.11 Model 5054 (MP.11a) Subscriber Unit – US/CAN PSU- World

Caribbean and Latin America Region

Base Station Unit

Part Number	Description
5054-BSU-US	Tsunami MP.11 Model 5054 (MP.11a) Base Station Unit - US/CAN PSU
5054-BSU-BR	Tsunami MP.11 Model 5054 (MP.11a) Base Station Unit - Brazil PSU

Residential Subscriber Unit

Part Number	Description
5054-RSU-US-WA	Tsunami MP.11 Model 5054 (MP.11a) Residential Subscriber Unit – US/CAN PSU with12 dBi Window Antenna
5054-RSU-BR-WA	Tsunami MP.11 Model 5054 (MP.11a) Residential Subscriber Unit – Brazil PSU with12 dBi Window Antenna
5054-RSU-US-MP	Tsunami MP.11 Model 5054 (MP.11a) Residential Subscriber Unit – USA/CAN - 5 pack*
5054-RSU-BR-MP	Tsunami MP.11 Model 5054 (MP.11a) Residential Subscriber Unit – Brazil PSU - 5 pack*

* 5-Packs contain: RSU (5), Power Supply (5); no software, no documentation, no antennas

Subscriber Unit

Part Number	Description
5054-SU-US-WA	Tsunami MP.11 Model 5054 (MP.11a) Subscriber Unit – US/CAN PSU
5054-SU-BR-WA	Tsunami MP.11 Model 5054 (MP.11a) Subscriber Unit – Brazil PSU

Accessories

Surge Arrestors/Cables

Part Number	Description
5054-SURGE	Surge Arrestor 0-6 GHz - Standard-N Female to Female
848 274 171	20 ft Low Loss Antenna Cable St-N - Male-Male LMR 200
848 332 789	20 ft Low Loss Antenna Cable St-N - Male-Male LMR 400
5054-ULA400-50	50 ft Low Loss Antenna Cable St-N - Male-Male LMR 400
848 274 205	75 ft Low Loss Antenna Cable St-N - Male-Male LMR 400
69828	6 ft Low Loss Antenna Cable St-N - Male-Male LMR 600
5054-LMR600-50	50 ft Low Loss Antenna Cable St-N - Male-Male LMR 60

5 GHz Antennas

Part Number	Description
5054-WA-15-STN	15 dBi Window Antenna
5054-PA-18	18 dBi Panel Antenna - St-N Female - 5.25 - 5.875 GHz
5054-PA-23	23 dBi Panel Antenna - St-N Female - 5.725 - 5.875 GHz
5054-OA-8	8 dBi Omni Directional Antenna - St-N Female - 5.47-5.850 GHz

Part Number	Description
5054-OA-10	10 dBi Omni Directional Antenna - St-N Female - 5.47-5.850 GHz
5054-SA120-14	14 dBi Sector Antenna - St-N Female - 5.25-5.850 GHz - 120 degrees
5054-SA60-17	17 dBi Sector Antenna - St-N Female - 5.25-5.850 GHz - 60 degrees

Power Injector

Part Number	Description
4312-XX	AE 3af 12 Port DC Injector
4306-XX	AE 3af 6 Port DC Injector
4301-XX	AE 3af 1 Port DC Injector

Outdoor Ethernet Cables

Part Number	Description
69819	25m outdoor, terminated CAT5 cable for Tsunami MP.11 or QB.11 with three RJ-45 and one weather-proof Ethernet port cap
69820	50m outdoor, terminated CAT5 cable for Tsunami MP.11 or QB.11 with three RJ-45 and one weather-proof Ethernet port cap
69821	75m outdoor, terminated CAT5 cable for Tsunami MP.11 or QB.11 with three RJ-45 and one weather-proof Ethernet port cap

Regulatory Approval and Frequency Ranges

Region/Country	Country	GHz	Number of Channels	Certification
North America	USA	5.25 - 5.35	Up to 14	Yes*
		5.47 - 5.725	Up to 14	Yes*
		5.725 - 5.85	Up to 5	Yes
	Canada	5.25 - 5.35	Up to 14	Yes†
		5.47 - 5.725	Up to 14	Yes†
		5.725 - 5.85	Up to 5	Yes
	Mexico	5.725 - 5.85	Up to 5	Yes

Region/Country	Country	GHz	Number of Channels	Certification
EU Countries	Austria	5.47 - 5.70	Up to 11	Yes
	Belgium	5.47 - 5.70	Up to 11	Yes
	Cyprus	5.47 - 5.70	Up to 11	Yes
	Czech Republic	5.47 - 5.70	Up to 11	Yes
	Denmark	5.47 - 5.70	Up to 11	Yes
	Estonia	5.47 - 5.70	Up to 11	Yes
	Finland	5.47 - 5.70	Up to 11	Yes
	France	5.47 - 5.70	Up to 11	Yes
	Germany	5.47 - 5.70	Up to 11	Yes
	Greece	5.47 - 5.70	Up to 11	Yes
	Hungary	5.47 - 5.70	Up to 11	Yes
	Ireland	5.47 - 5.70	Up to 11	Yes
		5.725 - 5.85	Up to 4	
	Italy	5.47 - 5.70	Up to 11	Yes
	Latvia	5.47 - 5.70	Up to 11	Yes
	Lithuania	5.47 - 5.70	Up to 11	Yes
	Luxemburg	5.47 - 5.70	Up to 11	Yes
	Malta	5.47 - 5.70	Up to 11	Yes
	Netherlands	5.47 - 5.70	Up to 11	Yes
	Poland	5.47 - 5.70	Up to 11	Yes
	Portugal	5.47 - 5.70	Up to 11	Yes
	Slovakia	5.47 - 5.70	Up to 11	Yes
	Slovenia	5.47 - 5.70	Up to 11	Yes
	Spain	5.47 - 5.70	Up to 11	Yes
	Sweden	5.47 - 5.70	Up to 11	Yes
	United Kingdom	5.47 - 5.70	Up to 11	Yes
		5.725 - 5.85	Up to 4	
Other European Countries	Iceland	5.47 - 5.70	Up to 11	Yes
	Liechtenstein	5.47 - 5.70	Up to 11	Yes
	Norway	5.47 - 5.70	Up to 11	Yes
	Russia	5.15 - 6.08	Up to 47	Yes
	Switzerland	5.47 - 5.70	Up to 11	Yes
South America	Argentina	5.25 - 5.35	Up to 3	Yes
		5.725 - 5.85	Up to 5	
	Brazil	5.47 - 5.70	Up to 11	Yes
		5.725 - 5.85	Up to 5	
	Colombia	5.25 - 5.35	Up to 3	Yes
		5.725 - 5.85	Up to 5	

Region/Country	Country	GHz	Number of Channels	Certification
APAC	Australia	5.725 - 5.85	Up to 5	Yes
	China	5.725 - 5.85	Up to 5	Yes
	Hong Kong	5.725 - 5.85	Up to 5	Yes
	India	5.15 - 5.35	Up to 8	Yes
		5.725 - 5.85	Up to 7	
	New Zealand	5.725 - 5.85	Up to 5	Yes
	S. Korea	5.725 - 5.85	Up to 5	Yes
	Singapore	5.15 - 5.25	Up to 4	Yes
		5.725 - 5.85	Up to 5	
	Taiwan	5.25 - 5.35	Up to 3	Yes
		5.725 - 5.85	Up to 5	

* FCC DFS in process.

† IC DFS in process.

OFDM Modulation Rates

NOTE: *Maximum packet size: 1526 Bytes*

Modulation	Rate
	20 MHz Channels
BPSK	6 and 9 Mbps
QPSK	12 and 18 Mbps
16-QAM	24 and 36 Mbps
64-QAM	48 and 54 Mbps

Wireless Protocol

Category	Specification
Wireless Protocol	Worp (Wireless Outdoor Router Protocol

Interfaces

Category	Specification
Wired Ethernet	Auto-sensing 10/100BASE-TX Ethernet
Serial Connector	RS-232
Antenna Connector for BSU/SU with Type N Connector	Standard Type-N Female

Receive Sensitivity

NOTE: *BER=10-6*

NOTE: *Rx Sensitivity values will have a tolerance of +/- 2 dB.*

Modulation	40 MHz Channels Turbo Mode (Non-DFS US Only)	20 MHz Channels Standard Mode
64QAM ¾	-66 dBm @ 108 Mbps	-69 dBm @ 54 Mbps
64QAM ½	-68 dBm @ 96 Mbps	-72 dBm @ 48 Mbps
16QAM ¾	-75 dBm @ 72 Mbps	-77 dBm @ 36 Mbps
16QAM ½	-78 dBm @ 48 Mbps	-80 dBm @ 24 Mbps
QPSK ¾	-81 dBm @ 36 Mbps	-83 dBm @ 18 Mbps
QPSK ½	-83 dBm @ 24 Mbps	-86 dBm @ 12 Mbps
BPSK ¾	-84 dBm @ 18 Mbps	-87 dBm @ 9 Mbps
BPSK ½	-85 dBm @ 12 Mbps	-88 dBm @ 6 Mbps

Maximum Throughput

Data Rate	40 MHz Channels Turbo Mode (US Non-DFS Only)	20 MHz Channels Standard Mode
108 Mbps Turbo 54	35 Mbps	—
96 Mbps Turbo 48	35 Mbps	—
72 Mbps Turbo 36	35 Mbps	—
48 Mbps Turbo 24	27 Mbps	—
36 Mbps Turbo 18	22 Mbps	—
24 Mbps Turbo 12	16 Mbps	—
54 Mbps	—	33 Mbps
48 Mbps	—	32 Mbps
36 Mbps	—	27 Mbps
24 Mbps	—	19 Mbps
18 Mbps	—	14 Mbps
12 Mbps	—	9 Mbps
9 Mbps	—	7 Mbps
6 Mbps	—	5 Mbps

Latency

Category	Specification
Typical at Max Throughput	10 ms (as measured with test equipment under controlled lab conditions and best performing packet size)

Transmit Power Settings

- Output Power Attenuation: 0 - 18 dB, in 1 dB steps

- Output Power Values will have a tolerance of +- 1.5 dB

Frequency	6-24 Mbps @ 20 MHz 16QAM ½; QPSK ¾; QPSK ½; BPSK ¾; BPSK ½
5.25-5.35 GHz	16 dBm
5.47-5.725 GHz	16 dBm
5.725-5.850 GHz	16 dBm

Range Information

NOTE: *PMP configuration using USA regulations for L and U bands, ETSI regulations for M bands. Clear LOS. Sector antenna (17 dBi, 60-degrees) at BSU with short 1 dB jumper cable. 3' parabolic dish (31.4 dBi) with short 1 dB jumper cable for SUs with external antennas. Fade margin minimum of 10 dB to 2 miles, 0.2 dB additional fade margin for every 0.1 mile to 15 dB*

External Antenna

Frequency	36 Mbps	6 Mbps
5.25-5.35 GHz (US)	1.1 mi/1.8 km	3.0 mi/4.8 km
5.47-5.725 GHz (ETSI)	1.0 mi/1.6 km	2.9 mi/4.7 km
5.725-5.850 GHz (US)	4.4 mi/7.1 km	12.2 mi/19.6 km

Hardware Specifications

Category	Specification
Radio	On-board 5 GHz radio
Processor	166 MHz Motorola 8241 processor
Memory	Flash: 8 MB; RAM: 16 MB

Software Features

Category	Specification
Key Features	• WORP protocol • Dynamic Data Rate Selection (Configured on BSU) • Transmit Power Control • Antenna Alignment (CLI output) • Integrity Check for Software Upload • Mobility with Auto-scanning • QoS Support; up to 8 classes of service, up to 8 service flows per class (BSU only) • Satellite Density • Enhanced Dynamic Frequency Selection (Configured on BSU) • Redundancy • Spanning Tree (802.1D)

Category	Specification
Bridging and Routing	• Bridge (802.1d) • IP/ RIPv1 (RFC 1058) • IP/ RIPv2 (RFC 1388) • CIDR (RFC 1519) • ICMP (RFC 792) • IP (RFC 791) • ARP (RFC 826)
Filtering	• Ethernet protocol (Ethertype) • Static MAC • Storm threshold • IP address • Broadcast protocol • Intra Cell Blocking (Configured on BSU)
Services	• DHCP Server (RFC 2131) • DHCP Client (RFC 2131) • Bi-Directional Bandwidth Control • NAT (RFC 3022) (Configured on SU) • DHCP Relay (RFC 2131) (Configured on SU)
VLAN	• 802.1Q (Configured on BSU)
Security Features	• Critical feature support via WORP for secure long-range wireless deployments in unlicensed frequency spectrum • MD5 (embedded in WORP) authentication between BSU and SU • Filter based on packet information such as unicast/multicast/ broadcast MAC or IP • MAC Authentication (Configured on BSU) • Secure “over the air encryption” with WEP, WEP+, and AES, and AES-CCB • RADIUS MAC Access Control (Configured on BSU) • RADIUS (RFC 2138) • Intra-cell blocking to allow the BSU to act as the central policy enforcer for SU to SU communications

Management

Category	Specification
Local	RS-232 serial (RJ-11, DB-9)
Remote	Web GUI, Telnet, TFTP, Link Test, SU/BSU Statistics, remote reboot/reload
SNMP	SNMPv1/v2; MIB-II; Ethernet-like MIB; BridgeMIB; 802.11 MIB; Private MIB; ORiNOCO MIB; RFC 1157; RFC 1213; RFC 1643; RFC 1493; RFC 2668

LEDs

Category	Specification
Types	• Power • Wireless Activity • Ethernet Activity

Power Requirements

Category	Specification
Power Adaptor (Wall Mount) (included)	• Input: 100 - 240 VAC, 0.4 Watts • Output: 12 VCD, 1.5 A • Power Consumption: Max 10 W
Power-over-Ethernet	• 802.3af compliant. Requires Power Injector or other 802.3af device • Input: Voltage 42 - 60 VDC • Output: Current 200 mA at 48 V
Power Consumption	Max 10 W

Physical and Environmental Specifications

Category	Specification
Physical	
Dimensions (H x W x D)	8.46 in x 6.89 in x 1.57 in (215 mm x 175 mm x 40 mm)
Weight	2.38 lbs (1.08 kg)
Environmental	
Storage Temperature	-20°C to 75°C
Operating Temperature	0°C to 55°C
Humidity	95% (non-condensing)

MTBF and Warranty

Category	Specification
MTBF	>100,000 hours
Warranty	1 year parts and labor

C

Lightning Protection

Lightning protection is used to maximize the reliability of communications equipment by safely re-directing current from a lightning strike or a power surge traveling along the Cat 5 Ethernet cabling to ground using the shortest path possible. Designing a proper grounding system prior to installing any communications equipment is critical to minimize the possibility of equipment damage, void warranties, and cause serious injury.

The surge arrestor (sometimes referred to as a lightning protector) can protect your sensitive electronic equipment from high-voltage surges caused by discharges and transients at the PoE.

Proxim Wireless offers superior lightning and surge protection for Tsunami MP.11 and Tsunami QuickBridge.11 products. Contact your reseller or distributor for more information.

Technical Services and Support

D

Obtaining Technical Services and Support

If you are having trouble utilizing your Proxim product, please review this manual and the additional documentation provided with your product.

If you require additional support and would like to use Proxim's free Technical Service to help resolve your issue, please be ready to provide the following information before you contact Proxim's Technical Services:

- **Product information:**
  - Part number of suspected faulty unit
  - Serial number of suspected faulty unit
- **Trouble/error information**:
  - Trouble/symptom being experienced
  - Activities completed to confirm fault
  - Network information (what kind of network are you using?)
  - Circumstances that preceded or led up to the error
  - Message or alarms viewed
  - Steps taken to reproduce the problem
- **Servpak information (if a Servpak customer)**:
  - Servpak account number
- **Registration information**:
  - If the product is not registered, date when you purchased the product
  - If the product is not registered, location where you purchased the product

NOTE: *If you would like to register your product now, visit the Proxim eService Web Site at* http://support.proxim.com *and click on* **New Product Registration**.

Support Options

Proxim eService Web Site Support

The Proxim eService Web site is available 7x24x365 at http://support.proxim.com.

On the Proxim eService Web Site, you can access the following services:

- **New Product Registration**: Register your product for free support.
- **Open a Ticket or RMA**: Open a ticket or RMA and receive an immediate reply.
- **Search Knowledgebase**: Locate white papers, software upgrades, and technical information.
- **ServPak (Service Packages)**: Receive Advanced Replacement, Extended Warranty, 7x24x365 Technical Support, Priority Queuing, and On-Site Support.
- **Your Stuff**: Track status of your tickets or RMAs and receive product update notifications.
- **Provide Feedback**: Submit suggestions or other types of feedback.
- **Customer Survey**: Submit an On-Line Customer Survey response.
- **Repair Tune-Up**: Have your existing Proxim equipment inspected, tested, and upgraded to current S/W and H/W revisions, and extend your warranty for another year.

Telephone Support

Contact technical support via telephone as follows:

- **Domestic**: 866-674-6626
- **International**: +1-408-542-5390

Hours of Operation

- **North America**: 8 a.m. to 5 p.m. PST, Monday through Friday
- **EMEA**: 8 a.m. to 5 p.m. GMT, Monday through Friday

ServPak Support

Proxim understands that service and support requirements vary from customer to customer. It is our mission to offer service and support options that go above-and-beyond normal warranties to allow you the flexibility to provide the quality of service that your networks demand.

In recognition of these varying requirements we have developed a support program called ServPak. ServPak is a program of Enhanced Service Options that can be purchased individually or in combinations to meet your needs.

- **Advanced Replacement**: This service offers customers an advance replacement of refurbished or new hardware. (Available in the U.S., Canada, and select countries. Please inquire with your authorized Proxim distributor for availability in your country.)
- **Extended Warranty**: This service provides unlimited repair of your Proxim hardware for the life of the service contract.
- **7x24x365 Technical Support**: This service provides unlimited, direct access to Proxim's world-class technical support 24 hours a day, 7 days a week, 365 days a year.
- **Priority Queuing**: This service allows your product issue to be routed to the next available Customer Service Engineer.

To purchase ServPak support services, please contact your authorized Proxim distributor. To receive more information or for questions on any of the available ServPak support options, please call Proxim Support at +1-408-542-5390 or send an email to servpak@proxim.com.

E

Statement of Warranty

Warranty Coverage

Proxim Wireless Corporation warrants that its Products are manufactured solely from new parts, conform substantially to specifications, and will be free of defects in material and workmanship for a Warranty Period of **1 year** from the date of purchase.

Repair or Replacement

In the event a Product fails to perform in accordance with its specification during the Warranty Period, Proxim offers return-to-factory repair or replacement, with a thirty (30) business-day turnaround from the date of receipt of the defective Product at a Proxim Wireless Corporation Repair Center. When Proxim Wireless has reasonably determined that a returned Product is defective and is still under Warranty, Proxim Wireless shall, at its option, either: (a) repair the defective Product; (b) replace the defective Product with a refurbished Product that is equivalent to the original; or (c) where repair or replacement cannot be accomplished, refund the price paid for the defective Product. The Warranty Period for repaired or replacement Products shall be ninety (90) days or the remainder of the original Warranty Period, whichever is longer. This constitutes Buyer's sole and exclusive remedy and Proxim Wireless's sole and exclusive liability under this Warranty.

Limitations of Warranty

The express warranties set forth in this Agreement will not apply to defects in a Product caused; (i) through no fault of Proxim Wireless during shipment to or from Buyer, (ii) by the use of software other than that provided with or installed in the Product, (iii) by the use or operation of the Product in an application or environment other than that intended or recommended by Proxim Wireless, (iv) by modifications, alterations, or repairs made to the Product by any party other than Proxim Wireless or Proxim Wireless's authorized repair partners, (v) by the Product being subjected to unusual physical or electrical stress, or (vii) by failure of Buyer to comply with any of the return procedures specified in this Statement of Warranty.

Support Procedures

Buyer should return defective LAN[1] Products within the first 30 days to the merchant from which the Products were purchased. Buyer can contact a Proxim Wireless Customer Service Center either by telephone or via web. Calls for support for Products that are near the end of their warranty period should be made not longer than seven (7) days after expiration of warranty. Repair of Products that are out of warranty will be subject to a repair fee. Contact information is shown below. Additional support information can be found at Proxim Wireless's web site at http://support.proxim.com.

- **Domestic**: 866-674-6626
- **International**: +1-408-542-5390

Hours of Operation

- **North America:** 8 a.m. to 5 p.m. PST, Monday through Friday
- **EMEA:** 8 a.m. to 5 p.m. GMT, Monday through Friday

When contacting the Customer Service for support, Buyer should be prepared to provide the Product description and serial number and a description of the problem. The serial number should be on the product.

In the event the Customer Service Center determines that the problem can be corrected with a software update, Buyer might be instructed to download the update from Proxim Wireless's web site or, if that's not possible, the update will be sent to Buyer. In the event the Customer Service Center instructs Buyer to return the Product to Proxim Wireless for

1. LAN products include: ORiNOCO™

repair or replacement, the Customer Service Center will provide Buyer a Return Material Authorization (“RMA”) number and shipping instructions. Buyer must return the defective Product to Proxim Wireless, properly packaged to prevent damage, shipping prepaid, with the RMA number prominently displayed on the outside of the container.

Calls to the Customer Service Center for reasons other than Product failure will not be accepted unless Buyer has purchased a Proxim Wireless Service Contract or the call is made within the first thirty (30) days of the Product’s invoice date. Calls that are outside of the 30-day free support time will be charged a fee of $25.00 (US Dollars) per Support Call.

If Proxim Wireless reasonably determines that a returned Product is not defective or is not covered by the terms of this Warranty, Buyer shall be charged a service charge and return shipping charges.

Other Information

Search Knowledgebase

Proxim Wireless stores all resolved problems in a solution database at the following URL: http://support.proxim.com.

Ask a Question or Open an Issue

Submit a question or open an issue to Proxim Wireless technical support staff at the following URL: http://support.proxim.com/cgi-bin/proxim.cfg/php/enduser/ask.php.

Other Adapter Cards

Proxim Wireless does not support internal mini-PCI devices that are built into laptop computers, even if identified as "ORiNOCO" devices. Customers having such devices should contact the laptop vendor's technical support for assistance.

For support for a PCMCIA card carrying a brand name other than Proxim, ORiNOCO, Lucent, Wavelan, or Skyline, Customer should contact the brand vendor's technical support for assistance.